Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Education for Pure Sciences
Department of Mathematics

Reliability of Asymmetric Cryptosystems

A Thesis
Submitted to the council of the College of Education for Pure Sciences
University of Babylon
as partial Fulfillment of the Requirements for the
Degree of Master in Education / Mathematics

By

Ban Jasim Kadhim Deccan

Supervised by

Asst. Prof. Dr. Ruma Kareem K. Ajeena

2023 A.D **1445 A.H**

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿هُوَ الَّذِي بَعَثَ فِي الْأُمِّيِّينَ رَسُولًا مِّنْهُمْ يَتْلُو عَلَيْهِمْ آيَاتِهِ وَيُزَكِّيهِمْ وَيُعَلِّمُهُمُ
الْكِتَابَ وَالْحِكْمَةَ وَإِن كَانُوا مِن قَبْلُ لَفِي ضَلَالٍ مُّبِينٍ﴾

سورة الجمعة – اية 2

Dedication

To the one who honored me by bearing his name,
my father, may Allah have mercy on him.
to the star of my life, my mother.
to everyone who taught me a letter.
to everyone who supported me, even with a smile.

Ban jasim

2023

Acknowledgements

My thanks and gratitude are to the gracious God who honored me by completing my studies

Many thanks are to my supervisor, Asst. Prof. Dr. Ruma Kareem K. Ajeena, for all that she presented to me, and my thanks and gratitud are to all my professors for their valuable efforts.

Contents

List of Figures

Figure No. **Title of Figure**

List of Tables

Table No. **Title of Table**

Mathematica Symbols

F	Field.
p	Prime number.
F_p	Prime field.
GF	Galois field.
G	generator element.
a, b	Privat keys.
k	Ephemeral key.
m_i	Plaintext messages.
C_i	Ciphertexts.
$\equiv$	Congruence.
R	Reliability.
$\mathrm{R_S}$	System Reliability.
Pr	probability.
Gcd	Greatest common divisor.
Mod	Modulo.
2 D	Two Dimension.
n D	n Dimension.
PK_{A_i}	Public key.

Abbreviations

EEA	Extended Euclidean Algorithm.
DLP	Discrete Logarithm Problem.
CRT	Chinese Remainder Theorem.
SS	Series System.
P-SS	Parallel-series system.
PS	Parallel System.
PTM	Path Tracing Method.
PSRM	Parallel-series Reduction Method.
PDM	Pivotal Decomposition Method.
EPKC	El-Gamal Public Key Cryptosystem.
RSA	Rivest–Shamir–Adleman.
RPKC	Rabin Public Key Cryptosystem.
R-EPKC	Reliable El-Gamal Public Key Cryptosystem.
R-RSA	Reliable RSA Public Key Cryptosystem.
R-RPKC	Reliable Rabin Public Key Cryptosystem.
PD-RSA	Pivotal Decompose RSA Public Key Cryptosystem
PD-EPKC	Pivotal Decompose El-Gamal Public Key Cryptosystem
PD-RPKC	Pivotal Decompose Rabin Public Key Cryptosystem

Publications

The publications of this work are

1. Ban Jasim K. Aljanaby & Ruma Kareem K. Ajeena, Reliable Rabin Cryptosystem Using the Modified Decomposition Method, Fourth International Conference on Advances in Physical Sciences and Materials 2023 (ICAPSM2023) organized by KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India, AIP Publishing, (Accepted).

2. Ban Jasim K. Aljanaby & Ruma Kareem K. Ajeena, Reliable Public Key Cryptosystem Type El-Gamal International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI 2023) scheduled to be held at KSR College of Engineering, Tiruchengode, Tamil Nadu, India during 19 - 20, October 2023, IEEE Publishing, (Accepted).

3. Ban Jasim K. Aljanaby & Ruma Kareem K. Ajeena, Reliable Reliable RSA Public Key Cryptosystem Using the Path Tracing Method, International Research Conference on Engineering and Applied Sciences 2023 (IRCEAS2023) organizing by College of Engineering in Al-Iraqia University in cooperation with Imam Ja'afar Al-Sadiq University (IJSU) in Iraq, and all accepted papers will publish in AIP Publishing, (Submitted).

Abstract

The security level in modern realities is very important and is designed to ensure confidentiality on the one hand and, on the other hand, full transparency of information. Reliability is related to availability which is described as the ability of a component or system to work at a specific moment or time interval. In this regard, this thesis aims to increase the level of security in asymmetric encryption algorithms such as the El-Gamal, RSA and the Rabin public key cryptosystems by relying on reliability methods. In the reliable versions of El-Gamal, RSA and Rabin public key cryptosystems were proposed with 2-dimension. On reliable El-Gamal, RSA and Rabin public key cryptosystems R-EPKC, R-RSA and R-RPKC respectively, the plaintext M is divided into two parts m_1 and m_2. Each part is encrypted independently to create two paths of the sub-ciphertexts. The ciphertext in the reliable proposed cryptosystems is represented by the network system consisting of two paths. The first path contains the ciphertext of m_1 and the second one contains ciphertext of m_2. The reliability of the proposed R-EPKC, R-RSA and R-RPKC is determined using the path tracing method (PTM). New technique for combining encrypted plaintext in two parts has been used with a reliable method that is called parallel-series reduction method (PSRM) which is employed for decrypting the ciphertext and recovering the original plaintext.

On the proposed 2- dimension of EPKC, RSA and RPKC another new contribution is applied using the modified pivotal decomposition method (M-PDM) (which is also named by modified conditional probability approach (M-CPA)). Using M-PDM, if one path from two sub-ciphertexts fails through the break down by attacker then it is possible to create a new path with a new sub-ciphertext. The M-PDM in compason with the original PDM deletes the failure path (that is attacked path) and changse it through creating new sub-ciphertext path. Even if the attacker recovers one part of the plaintext m_1 or m_2, he/she cannot obtain all the information in the original plaintext, only part of it, and therefore he/she does not benefit from the information he/she obtained.

In comparsion with the proposed reliable cryptosystems, the ciphertext in the original cryptosystems has only one path as a series, and if it fails of one of the components of the path means that the ciphertext fails, whereas, dividing the

plaintext into two parts, the reliable system will become parallel and the failure of one part of the system does not mean the failure of the entire system. Also, the proposed cryptosystems have been generalized to *n*-dimension. The goal of dividing the plaintext into *n* parts is to obtain higher system reliability that increases the security of the proposed cryptosystems.

New experimental results of R-EPKC, R-RSA and R-RPKC are discussed as study cases with small parameters. The security considerations on R-EPKC, R-RSA and R-RPKC are determined. Using the PTM, PSRM and M-PDM, the R-EPKC, R-RSA and R-RPKC are considered as more secure cryptosystems for communication in comparsion to the original ones.

Chapter One

Introduction

Introduction

1.1 General Introduction

Security and reliability aspects became an indivisible part of data transfer. Both aspects have received special interest from researchers and scholars in the near past. Reliability is largely achieved by the use of total probability theory techniques and security by cryptographic techniques. A ppropriate combination of techniques of total probability theory and cryptography will make it possible to achieve the goals of reliable and secure communication [1].

The main important point on which encryption protocols are based is to make confidential data incomprehensible to unauthorized persons. One of the most common uses is to transfer data over an insecure channel such as the Internet. In this case, the fact of encrypted information does not prevent unauthorized persons from accessing it, but ensures that they do not understand the meaning [2].

These schemes are designed based on some mathematical problems, one of them those are solved using the basic concepts of reliability methods. The connection between some reliability methods and the encryption protocols is made in this thesis. By creating new models, the basic basis of which is the structure function of reliability schemes in drawing the paths of the ciphertext sent between users. New versions of asymmetric cryptographic algorithms are proposed based on the transfer of plaintext to n-dimension by dividing it into n-parts. The security issues of the proposed schemes are determined using one of the reliability methods. Two study cases are presented: reducing the plaintext after the decryption process to retrieve the original plaintext, deleting the path exposed to hacking, and creating a new alternative path. On proposed schemes, the ciphertexts of the plaintexts are sent to the receiver entity. The R-EPKC, R-RSA, R-RPKC, PD-EPKC, PD-RSA, and PD-RPKC schemes are considered new insights for more secure communications.

1.2 Previous Studies

Several researchers employed concepts of mathematical to modify the encryption schemes and make them more secure for communications.

In 2006, Breveglieri, L. [3] proposed the classical reliability modeling techniques to cryptographic systems, introducing concepts like Cryptographic Key Failure Tolerance and Cryptographic Key Reliable Lifetimes. It provides a framework for determining reliable lifetimes of keys in the presence of faults, with an acceptable error-bound for key exposure risk. Emphasizes the importance of selecting keys with good failure tolerance and recommends minimal values.

In 2013, Iaremchuk. [4] proposed cryptographic methods based on public key technology require simplification and cryptographic reliability. Asymmetric encryption and encryption without prior key distribution are interesting methods. However, studying their cryptographic reliability and comparison with known analogues is crucial. A theory-and-complexity approach evaluates theoretical cryptographic reliability, revealing that attempts to break these methods are limited to the necessity of a more complex approach.

In 2014, Xiao et al. [5] proposed the usage of the reliability theory for evaluating and estimating the performance of key management schemes (KMSs). The analysis of reliability showed the KMSs concentrate on postponing the key theft as well as possible directions to improve the reliability of KMSs.

In 2015, Ahmadi, et al. [6] proposed a reliable user authentication and data protection model for cloud computing, utilizing AES and RSA encryption for enhanced security.

In 2017, Subramanian et al. [7] presented two block ciphers used for authenticated encryption algorithms. Also in their work, efficient error detection architectures with encoded operands and signature-based schemes to detect the transient and permanent faults are introduced to apply in cryptography for providing the confidentiality, integrity, and authenticity together for a plaintext sent over a communication channel.

In 2021, Çalkavur, [8] proposed examining network transaction security, reliability, SSL protocol structure, disadvantages, and proposed improvement measures.

In 2022, Akhatov et al. [9] presented their work to focus on the cryptographic methods using block chain. The block chain was used to enhance the RSA6 cryptographic technique and the D-RSA6 algorithms were formed.

1.3 Statement of the Problem

In this work, new versions of the encryption cryptosystems are proposed such as El-Gamal, RSA and Rabin. These cryptosystems are used for designing the alternative versions of cryptosystems based on the reliability systems to increase the security in compared to the original cryptosystems. The R-EPKC, R-RSA and R-RPKC are used to calculate the reliability of the new version scheme and reducation the plaintext after decrypting. The PD-EPKC, PD-RSA and PD-RPKC are used to delete the path exposed to hack and create a new replacement. The ASCII has also been used to encrypt English phrases with modified El-Gamal. On the proposed R-EPKC, R-RSA, R-RPKC, PD-EPKC, PD-RSA and PD-RPKC schemes, the security considerations are determined. More secure communications using the R-EPKC, R-RSA, R-RPKC, PD-EPKC, PD-RSA and PD-RPKC cryptosystems are investigated, so they are considered as new insights for communications.

1.4 Thesis Objectives

- Propose new versions of asymmetric cryptosystems in the 2-dimension which are R-EPKC, R-RSA, R-RPKC, PD-EPKC, PD-RSA and PD-RPKC.
- Use the PTM and M-PDM to calculate the reliability and to increase the security.
- Generalize the R-EPKC, R-RSA, R-RPKC, PD-EPKC, PD-RSA and PD-RPKC into *n*-dimension.

1.5 Thesis Structure

The outline of this study is as follows:

In addition to the introduction chapter, the outline consists of the following chapters

- **Chapter Two:** The first part includes encryption basics. The second part includes an explanation of the definitions of cryptography and some kinds the reliability, numbers and cryptosystem of the asymmetric encryption schemes. The last part includes some concepts of reliability theory through definitions, methods and examples.

- **Chapter Three:** It includes the proposition of new versions of reliable asymmetric cryptosystems in two dimensions that are named 2D-R-EPKC, 2D-R-RSA and 2D-R-RPKC. Using the PTM based on RSRM also, it includes the new versions of asymmetric encryption schemes. In the last part, it includes *n* dimensions of these versions of the asymmetric cryptosystems that are used same reliable methods. The security considerations for R-EPKC, R-RSA and R-RPKC are determined.
- **Chapter Four:** It includes the proposition of new versions of decomposed asymmetric encryption in two dimensions that are named 2D-PD-EPKC, 2D-PD-RSA and 2D-PD-RPKC that are emplayed the M-PDM. In the last part, it includes *n* dimensions of this version of the asymmetric cryptosystem with same relible method, namely M-PDM. The security considerations for PD-EPKC, PD-RSA and PD-RPKC are determined.

- **Chapter five:** Includes the numerical result, conclusions and future works.

Chapter Two

Mathematical Background

Of Reliability and

Cryptography

Mathematical Background of Reliability and Cryptosystem

2.1 Introduction

In this chapter, three asymmetric encryption algorithms will be presented. These protocols are used to encrypt data that is submitted over an unsecured channel. First, the El-Gamal algorithm, devised by Taher El-Gamal in 1985, which is used to encrypt the declared public key. The encryption of El-Gamal consists of three parts: a keys generator, an encryption algorithm, and a decryption algorithm. Second, the RSA algorithm is an acronym for Rivest-Shamir-Adleman. According to the scientists who created this algorithm, an asymmetric encryption algorithm based on a mathematical protocol that produces two keys, one public and one private. Third, Rabin algorithm: Rabin developed a public-key cryptosystem in 1979 whose security depends on the difficulty of computing square roots modulo an integer n. On the other hand, some methods of reliability will be introduced, which are used to compute the reliability of complex and simple systems. This is the path tracing method, the parallel-series reduction method, and the decomposition method. These methods are the basis for creating new, reliable encryption schemes.

2.2 Reliability

Definition 2.2.1 Reliability is the probability that the component will perform. its intended function for a certain time under stated conditions, the probability of successful or unsuccessful operation depends on the efficiency and power of the component [10].

Definition 2.2.2 The word "reliability" refers to performance that is successful, dependable, and effective. It's not only a vague concept for systems; it can be computed, measured, assessed, planned for, and created specifically for a system [11], [12].

2.3 Basic Facts

This section presents some fundamental facts and concepts related to the reliability systems.

2.3.1 Some Reliability Systems

There several reliability systems, some of them are discussed as follows.

2.3.2 Series Systems The success or failure of full system can be determined based on the components of it. With the failure of one or more than one component in the system and the result is a failure then the system is named by series system (SS) [13] as shown in Figure (2.1).

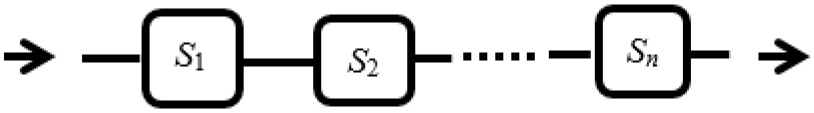


Figure 2.1. A series system (SS).

This means that, all components of the system work, so the system success to perform the function that designed for it. Let SS has *n* mutually independent components. The failure of one component, with mutually independence property, is not affecting on the life of the rest components. The parameters that can be used are: S_i is the event (path) with component *i* that is operational, *S* is the path of the system, *R* is the system reliability and *R_i* indicates to the reliability of component *i*. The system reliability is determined based on the probability by [14]

$$R = \Pr(S) = \Pr(S_1 \cdot S_2 \cdot \ldots\ldots \cdot S_n\ ). \tag{2.1}$$

Since the components are independent, so

$$\left.\begin{aligned} R &= \Pr(S) = \Pr(S_1)\cdot\Pr(S_2)\cdot\ldots\ldots\cdot\Pr(S_n) \\ &= \prod_{i=1}^{n} R_i\,. \end{aligned}\right\} \tag{2.2}$$

The system reliability is

$$R = R_0^n, \tag{2.3}$$

when all *n* components be identical to the reliability R_0 [15].

2.3.2 Parallel Systems.

If the failure of full system occurred depending on the failure that obtained all components of the system, so this system is called a parallel system that is shown in Figure (2.2) [16].

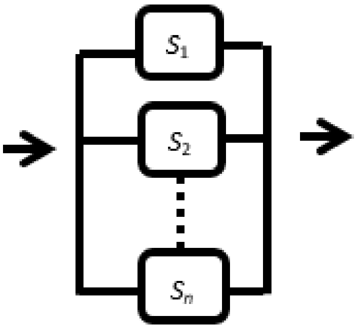


Figure 2.2. A Parallel System.

In general, the reliability of a parallel system can be computed as follows. With *n* components of a parallel system which are mutually independent components. The system unreliability F (failure probability) is expressed by [17]

$$F = \Pr(\bar{S}) = \Pr(\bar{S}_1 \cdot \bar{S}_2 \cdot \ldots \cdot \bar{S}_n), \tag{2.4}$$

where $\bar{S}$ is the complement element of *S*. Since the event (path) $\bar{S}_i$ are mutually impendent then *F* in Equation (2.4) can be rewritten by

$$\left.\begin{aligned} F &= \Pr(\bar{S}) = \Pr(\bar{S}_1)\cdot\Pr(\bar{S}_2)\cdot\ldots\cdot\Pr(\bar{S}_n) \\ &= \prod_{i=1}^{n}(1-R_i). \end{aligned}\right\} \tag{2.5}$$

The system unreliability components gives the system reliability, namely [18]

$$R = 1-\prod_{i=1}^{n}(1-R_i). \tag{2.6}$$

The identical of all components *n* leads to

$$R = 1-(1-R_0)^n \tag{2.7}$$

2.3.3 Parallel–Series System A parallel–series system consists of *m* disjoint modules that are connected in parallel and module *i* for $1 \le i \le m$ consists of n_i components that are connected in series.

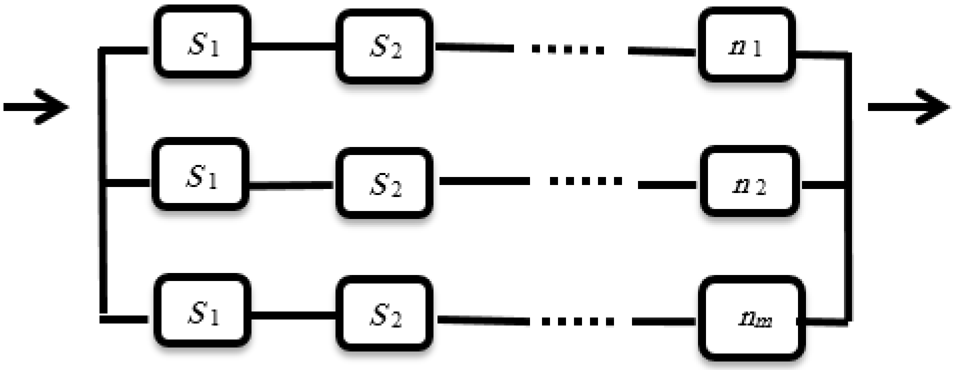


Figure 2.3. A parallel-series system.

The reliability block diagram of a parallel–series system is given in Figure (2.3). In such a parallel–series system, there are *m* minimal paths and they do not have any components in common. Using the technique of modular decomposition, we can first express the reliability of each module as a function of its component reliabilities and then the reliability of the system as a function of the reliabilities of the modules [19].

Notation

- p_{ij}: reliability of component j in module i, $1 \le i \le m$, $1 \le j \le n_i$

- q_{ij}: $1 - p_{ij}$, $1 \le i \le m$, $1 \le j \le n_i$

the reliability of module i is

$$P_i = \prod_{j=1}^{n_i} P_{ij} \text{ , } i = 1, 2, ..., m. \tag{2.8}$$

the reliability of a parallel–series system is

$$R_s = 1 - \prod_{j=1}^{m} (1 - P_i) = 1 - \prod_{i=1}^{m} (1 - \prod_{j=1}^{n_i} P_{ij}). \tag{2.9}$$

When the reliability $p_{ij} = p$ and the number of components in each module is constant, that is, $n_i = n$, the system reliability can be expressed as [20]

$$R_s = 1 - (1 - p_n)^m. \tag{2.10}$$

2.4 Some Reliable Methods of the complex systems

2.4.1 Path Tracing Method (PTM) [21].

Several methods are available for determining the reliability of a complex system that is given in Figure (2.4).

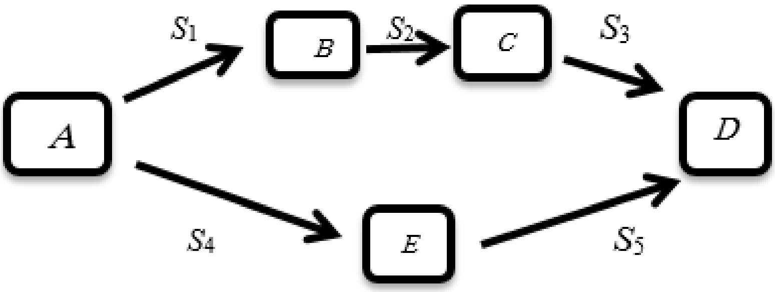


Figure 2.4. A parallel-series.

One of these method is the path tracing method (PTM). On PTM, each path from a starting point into an ending point can be considered. At least one path available from one end of the reliability block diagram to the other, [22] as long as at least one path from the beginning to the end of the path is available which determines the success of a system. So, the system is not failed. Assume starting and ending blocks that cannot fail as shown in Figure (2.5).

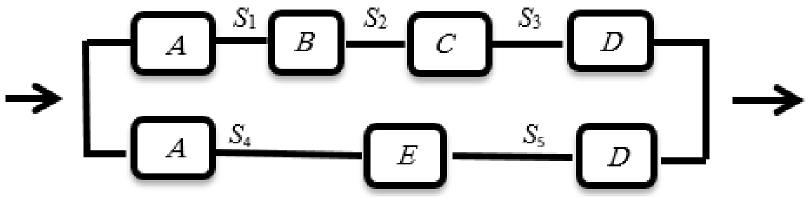


Figure 2.5. A parallel-series of complex system.

The minimal path for this system, in Figure (2.5), are: $P_1 = S_1S_2S_3$ and $P_2 = S_4S_5$. The reliability Rs_j with j=1,2 of series paths computes based on the reliability R_i of subsystems S_i for i=1,2,3,4,5. So, the reliability is computed as given in Equation (2.2) [23].

Based on Figure (2.5), one can compute

$$\begin{aligned} Rs_1 &= R_1R_2R_3 \\ Rs_2 &= R_4R_5. \end{aligned}$$

The reliability of parallel system R_p is determined as given in Equation (2.6)

$$\begin{aligned} Rs &= 1-\left[(1-Rs_1)(1-Rs_2)\right] \\ &= 1-\left[(1-R_1R_2R_3)(1-R_4R_5)\right] \\ &= R_4R_5 + R_1R_2R_3 - R_1R_2R_3R_4R_5. \end{aligned}$$

2.4.2 Parallel-Series Reduction Method (PSRM) [24]

The reliability block diagram of a complex system that is given in Figure (2.6) can be shown by

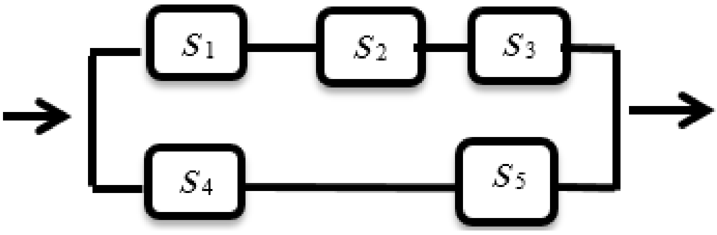


Figure 2.6. Block diagram.

The system has five components S_i, for i = 1,2,3,4,5. The reliability of component S is R_i. For evaluating the reliability of a system, it can use the series and parallel reduction method. Based on Figure (2.6), the system structure has a super-component S_a which consists of the components S_1, S_2 and S_3 that form a series subsystem. The reliability of a super-component S_a is equal to the product of the reliabilities of components S_1, S_2 and S_3 that is given by

$$R_a = R_1 R_2 R_3.$$

In similar way, the components S_4 and S_5 form a series subsystem which can be represented by a super-component S_b. The reliability of super-component S_b is equal to the product of the reliabilities of components S_4 and S_5 that is computed by $R_b = R_4 R_5$.

The super-components S_a and S_b form the series reductions of the block diagram in Figure (2.6) which are expressed as shown in Figure (3.7).

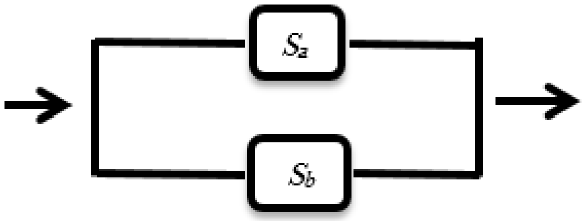


Figure 2.7. The series reductions of block diagram.

The reliability R_S of parallel system that is formed by super-componenst S_a and S_b is computed as given in Equation (2.6)

The super-components S_a and S_b form a parallel subsystem S_c. The reliability $R_c(t)$ is determined by

$$\begin{aligned} R_c &= 1 - \left[(1-R_a)(1-R_b)\right] \\ &= R_a + R_b - R_a R_b . \end{aligned}$$

The reliability block diagram in Figure (2.7) using the parallel reduction can be expressed as shown in Figure (2.8).

Figure 2.8. The parallel reduction of the super-components S_a and S_b.

2.4.3 Pivotal Decomposition Method (PDM)

In some cases, there are more complex systems, such as the well-known bridge system shown in Figure (2.9), that cannot be solved by the series-parallel reduction method [19]. This kind of system uses the pivotal decomposition method also known as the conditional probability approach. The decomposition method starts with selecting a keystone component, namely *A*, from the system being studied. This component appears to bind the system together. In Figure (2.9), e.g., component *A* is the keystone component. The keystone component is assumed to be fully reliable, which is why it is replaced with a line in the scheme of the system. Then the same component is supposed to fail and be deleted from the entire system. The system reliability is calculated according to the rule of total probability and can be written as

R_S = Pr(component *A* is success) Pr(system success\ component *A* is success) + Pr(component *A* is failure)Pr(system success\ component *A* is failure).

R_S = Pr(A)Pr(system success\ *A* success)+Pr($\overline{A}$)Pr(system success\ *A* success).

Consider the reliability of the system with the reliability block diagram shown in Figure (2.9). Also assume that the components are independent.

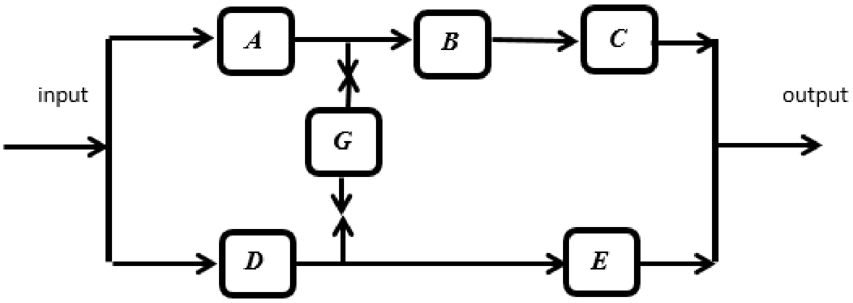


Figure 2.9. Block diagram model.

The calculations involved in evaluating the reliability of the complex system in Figure (2.9) using the decomposition method are explained as follows:

First step: select a keystone component. Here, choose component *G* as the keystone component because this choice will reduce the reliability block diagram to a series or parallel configuration or a combination of both in a single step.

Second step: Now, component *G* can be good or bad. The reduced subsystems corresponding to these cases are shown in Figure (2.10).

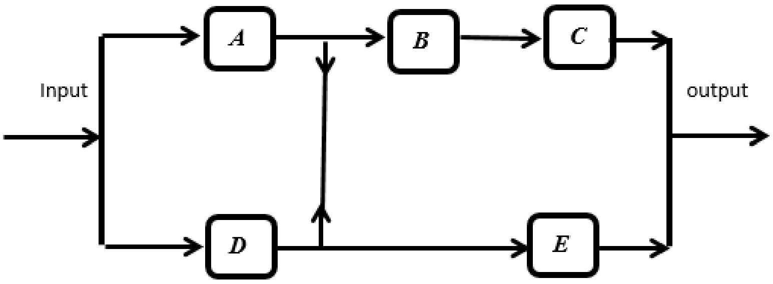


Figure 2.10. Complex system for success component *G*.

Three step: Let R_i denote the reliability of the component *i*, (*i* = *A*, *B*, *C*, *D*, *E*, *G*). In this step, we first evaluate the reliabilities of each reduced subsystem. Note that in subsystem, the components *A*, *D* are in parallel, components *B*, *C* and *E* are in parallel and the two parallel configurations are in series (see Figure (2.10)).

$$R_s = P \text{ (system success\ component } G \text{ is success)}$$

$$= [1\text{- } (1 - R_A)(1\text{- } R_B)(1\text{- } R_C)] \times [1\text{- } (1\text{-}R_D)\ (1\text{- } R_E)]$$

$$= (R_A + R_B + R_C – R_A R_B R_C) (R_D + R_C - R_A R_D)$$

In subsystem, the components *A*, *B* and *C* are in series, components *D* and *E* are in series and the two series configurations are in parallel (see Figure (2.11)).

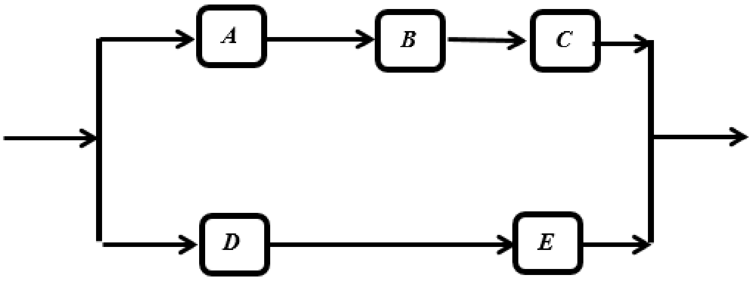


Figure 2.11. Complex system for failure component *G*.

$$R_S = P(\text{system success \textbackslash component } G \text{ is failure})$$

$$= [1-(1-R_A R_B R_C)(1- R_D R_E)] = R_A R_B R_C + R_D R_E - R_A R_B R_C R_D R_E$$

$$R_s = P(\text{system success\textbackslash\ component } G \text{ is success}) P(\text{component } G \text{ is success}) +$$
$$P(\text{system success\textbackslash\ component } G \text{ is failure}) P(\text{component } G \text{ is failure})$$

$$= R_G[(R_A + R_D - R_A R_D)(R_B + R_C + R_E -R_B R_C R_E)] +$$

$$(1- R_G)[R_A R_B R_C + R_D R_E - R_A R_B R_C R_D R_E)$$

2.5 Fields

In this section, the mathematical framework associated with fields, particularly finite fields, is discussed as follows:

Definition 2.5.1 (Field) A field *F*, sometimes denoted by (*F*, +, ×), is a set of elements with two binary operations, called addition and multiplication, such that for all *h*, *k*, and *m* in *F*, the following axioms are true:

1. Closure under addition and multiplication: If *h* and *k* belong to *F*, then $h + k$ and $h×k$ are also in *F*
2. Commutativity of addition and multiplication: $h + k = k + h$, $h×k = k×h$ for all *h*, *k* in *F*.

3. Associativity of addition and multiplication: $(h +k) + m = h + (k + m)$, $h \times (k \times m) = (h \times k) \times m$ for all h, k, m in F.

4.Distributive laws: $h \times (k + m) = h \times k + h \times m$ for all h, k, m in F.

$(h + k) \times m = h \times m + k \times m$ for all h, k, m in F.

5. Addition identity: There is an element 0 in F such that $h + 0 = 0 + h = h$ for all h in F. So, multiplicative identity: There is an element 1 in F such that $h \times 1 = 1 \times h = h$ for all h in F

7. Addition inverse: For each h in there is an element $(-h)$ in F such that $h + (-h) = (-h) + h = 0$. So, multiplicative inverse: For each h in F, except 0, there is an element h^{-1} in F such that $h \times (h^{-1}) = (h^{-1}) \times h = 1$[25].

Definition 2.5.2 (Finite Field or Galois Field) A field with a finite set is called a finite field. If a finite field has p number and p is prime, then the field is called a prime field. It can be shown that the order of a finite field must be a power of a prime p^n, where n is a positive integer. The finite field of order p^n is generally written $GF(p^{\mathrm{n}})$; GF stands for Galois field. The special case for $n = 1$, we have the finite field $GF(p)$; this finite field has a different structure than that for finite fields [26].

Definition 2.5.3 (finite field of order p) For a prime number p, define the finite field of order p, $GF(p)$, as the set Fp of integer numbers $\{0, 1, ..., p - 1\}$ prime field. The two operations of the field are modular integer addition and integer multiplication modulo p [25].

Definition 2.5.4 (Relatively Prime) [27] Two integers a and b, not both of which are zero, are said to be relatively prime whenever gcd(a, b) =1.

Definition 2.5.5 (Euler's totient function) [25] This function, written f(n), is defined as the number of positive integers less than n and relatively prime to n. By convention, Ø (1) = 1

$$Ø(N) = Ø(pq) = Ø(p) * Ø(q) = (p - 1) * (q - 1)$$

Definition 2.5.6 (quadratic residue)[25] An integer q is called a quadratic residue modulo n if it is congruent to a perfect square modulo n; i.e.,

$$x^2 \equiv q (\bmod n)$$

if there exists an integer x such that Otherwise, q is called a quadratic nonresidue modulo n.

2.5.7 Arithmetic operation on a Prime Field

The operations of arithmetical, multiplication, addition and subtraction, can be computed over a prime field F_p. For example with a small value let $p = 7$ can be given to explaining the arithmetic operation on F_7. The multiplication can be computed by

$$6 \times 5 \ (\bmod\ 7) \equiv 30 (\bmod 7) \equiv 2 (\bmod 7).$$

and the addition operation can be calculated by

$$6 + 5 \ (\bmod\ 7) \equiv 11 \ (\bmod\ 7) \equiv 4 \ (\bmod\ 7)$$

While, the subtraction done by

$$6 - 5 \ (\bmod\ 7) \equiv 1 \ (\bmod\ 7).$$

Now, what about calculating the division over F_p? and how to get the value of $h/k \ (\bmod\ p)$? The answer is: it is possible to calculating the division over F_p by calculating the inverse element modulo p which is given in the follows

$$\frac{h}{k} (\bmod p) \equiv h \frac{1}{k} (\bmod p) \qquad (2.11)$$

to calculating the inverse element mod p, there are some methods, one of these methods is the extended Euclidean algorithm (EEA) [28].

2.6 The Discrete Logarithm Problem in Prime Fields

The discrete logarithm problem is a mathematical problem that appear in many settings, including the mod *p*, the discrete logarithm problem (DLP), can directly be explained using cyclic groups. Startation with the DLP over F_p^*, where p is a prime[29].

Definition 2.6.1. (Discrete Logarithm Problem (DLP)). in F_p^* given is the finite cyclic group F_p^* of order p^{-1} and a primitive element $a \in F_p^*$ and another element $b \in F_p^*$ The DLP is the problem of determining the integer $1 \le x \le p - 1$ such that: $ax \equiv b \bmod p$.

This integer *x* is called the discrete logarithm of *b* to the base *a*, and we can formally write: $x = log_a\, b \bmod p$.

Computing discrete logarithms modulo a prime is a very hard problem if the parameters are sufficiently large. Since exponentiation $ax \equiv b \bmod p$ is computationally easy, this forms a one-way function

Example 2.6.2 consider the group F_{47}^* which has order 46. The subgroups in F_{47}^* have thus a cardinality of 23, 2 and 1. $a = 2$ is an element in the subgroup with 23 elements, and since 23 is a prime, *a* is a primitive element in the subgroup. A possible discrete logarithm problem is given for $b = 36$ (which is also in the subgroup): Find the positive integer *x*, $1 \le x \le 23$, such that $2^x \equiv 36 \pmod{47}$ By using a brute-force attack, obtained a solution for $x = 17$

Definition 2.6.3 Generalized Discrete Logarithm Problem Given is a finite cyclic group *G* with the group operation (◦) and cardinality *n* [29]. We consider a primitive element $a \in G$ and another element $b \in G$. The discrete logarithm problem is finding the integer *x*, where $1 \le x \le n$, such that:

$$b = \underbrace{a \cdot a \cdot a \cdot ..... \cdot a}_{xtimes} = a^x \tag{2.12}$$

Example 2.6.4 This time considered the additive group of integers modulo a prime. For instance, if chooses the prime $p = 11$, $G = (F_{11}, +)$ is a finite cyclic group with the primitive element $a = 2$. Here is how *a* generates the group:

tried not to solve the DLP for the element b = 3, i.e., have to compute the integer $1 \leq x \leq 11$ such that

$$2^x = \underbrace{2+2+2+.....+2}_{xtimes} \equiv 3(\mathrm{mod}11) \qquad (2.13)$$

Here is how an “attack” against this DLP works. Even though the group operation is addition, can express the relationship between a, b and the discrete logarithm x in terms of multiplication.:

$$2^x \equiv 3(mod11) \qquad (2.14)$$

In order to solve for x, simply have to invert the primitive element a:

$$x \equiv 2^{-1}3(mod11) \qquad (2.15)$$

Using, e.g., the extended Euclidean algorithm, can compute $2^{-1} \equiv (6 \bmod 11)$ form which the discrete logarithm follows as:

$$x \equiv 2^{-1}3 \equiv 7(mod11) \qquad (2.16)$$

2.7 Extended Euclidean Algorithm (EEA).

The Extended Euclidean algorithm (EEA) depends to compute the integers h and k such that

$$ah + bk = n = \gcd(a,b) \qquad (2.17)$$

where n is a greatest common divisor of a and b. The extended Euclidean algorithm not only computes the greatest common divisor but also for calculating the inverse element modulo p, where p is a prime number. Before discussing of this algorithm, we are needed to present some mathematical concepts as a basis to EEA [30].

2.7.1. (The Division Algorithm). Given any nonnegative integer m and n, if we divide n by m, we get an integer quotient q and an integer remainder r as shown in the equation:

$$n = qm + r \quad 0 \leq r < m; \quad q = \lfloor n / m \rfloor \qquad (2.18)$$

The largest integer less than or equal to x is $\lfloor x \rfloor$. The equation (2.8) namely the division algorithm [31].

Theorem 2.7.2 Let m and n be integers, not both zero. Then m and n are relatively prime if and only if there exist integers t and s such that $1 = mt + ns$ [32].

The Euclidean Algorithm can be described as follows.

Theorem 2.7.3 (The Euclidean Algorithm).[33] Let h and k be two integers such that $h \geq k > 0$. The first step is to apply the division algorithm, to h and k to get

$$h = q_1 k + r_1, \text{ with } 0 \leq r_1 < k.$$

If $r_1 = 0$, then $k \mid h$ and $\gcd(h,k) = k$. Whereas, if $r_1 \neq 0$, divide k by r_1 to produce integers q_2 and r_2 which satisfy

$$k = q_2 r_1 + r_2, \text{ with } 0 \leq r_2 < r_1.$$

If $r_2 = 0$, then it should stop. Otherwise, proceed as before to get

$$r_1 = q_3 r_2 + r_3, \text{ where } 0 \leq r_3 < r_2.$$

The division processing continues until getting a zero remainder. For instance, on the $(n+1)$ the stage, r_{n-1} is divided by r_n. A zero remainder appears, since the decreasing sequence $k > r_1 > r_2 > \ldots \geq 0$ cannot contain more than k integers. This process can be expressed by the system of the following equations:

$$\begin{array}{ll} h = q_1 k + r_1 & 0 \leq r_1 < k \\ k = q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \end{array}$$

.

.

$$r_{n-2} = q_n r_{n-1} + r_n \qquad\qquad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

The last nonzero remainder r_n is the $\gcd(h,k)$ [32].

Example 2.7.4 Suppose $h = 88$ and $k = 24$. The computation of $\gcd(88,24)$ by using the Euclidean algorithm can be done based on Theorem (2.6.3). The greatest common divisor of 88 and 24 is equal to 8.

In other words,

$$8 = \gcd(88,24)$$

For representing the positive integer 8 as a linear combination of the integers 88 and 24, the back substitution way can be used on the remainders 0,8 and 16.

Thus,

$$8 = \gcd(88,24) = 88t + 24s$$

where $t = 2$ and $s = -7$. There are other possibilities to write the positive integer 8 as a linear combination of 88 and 24. In other words, the values of t and s to express the positive integer 8 are not unique.

The back substitution way of the Euclidean algorithm to compute the values of t and s in the following relation

$$q = \gcd(h,k) = ht + ks$$

is known by the extended Euclidean algorithm (EEA). Algorithm (2.6) computes

$$ht_1 + kt_1 = y, ht_2 + kt_2 = x \text{ with } y \le x,$$

where $y = 0$, the EEA terminates. In this case $x = \gcd(h, k)$ and $t = t_2$, $s = s_2$ that satisfy $ht + ks = q$.

Algorithm 2.7.5 Extended Euclidean for integers [27].

Input: nonnegative integers h and k with $h \geq k$.

Output: $q = \gcd(h, k)$ and integers. $q = sk + th$, satisfying t, s

```
1. $x \leftarrow h, y \leftarrow k$
2. $t_1 \leftarrow 1, s_1 \leftarrow 0, t_2 \leftarrow 0, s_2 \leftarrow 1$
3. **While** $y \neq 0$ **do**
    3.1 $q \leftarrow \left\lfloor \frac{x}{y} \right\rfloor, r \leftarrow x - qy, t \leftarrow t_2 - qt_2, s \leftarrow s_2 - qs_1$.
    3.2 $x \leftarrow y, y \leftarrow r, t_2 \leftarrow t_1 \leftarrow t, s \leftarrow s_2 \leftarrow s_1 \leftarrow s$.
4. **End while**
5. $q \leftarrow y, t \leftarrow t_2, s \leftarrow s_2$.
6. **Return** $(q, r, t, s)$.
```

Example 2.7.6 Suppose h = 191 and k =81. The gcd(191,81) =1, since 191 and 81 are relatively prime. The goal here is to find the values of t, s and the remainders r using Algorithm (2.4.6).

Suppose $h = x$ 191, $k = y = 81$, and the initial values is t_1=1, s_1= 0, t_2 =0, s_2 =1.

Now, if $y = 81 \neq 0$ then

$$q = \left\lfloor \frac{191}{81} \right\rfloor = 2, r = 191 - 81 \times 2 = 29, t = 0 - 2 \times 1 = -2, s = 1 - 2 \times 0 = 1$$

So, $x = 81, y = 29, t_2 = 1, t_1 = -2, s_2 = 0, s_1 = 1$

When $y = 29 \neq 0$ then

$$q \left\lfloor \frac{81}{29} \right\rfloor = 2, r = 81 - 29 \times 2 = 23, t = 1 - (-2 \times 2) = 5, s = 0 - (-2 \times 1) = 2.$$

Therefore, $x = 29, y = 23, t_2 = -2, t_1 = 5, s_2 = 1, s_1 = 2.$

If y = 23 ≠0 then

$$q = \left\lfloor \frac{29}{23} \right\rfloor = 1, r = 29 - 23 \times 1 = 6, t = (-2) - 1 \times 5 = -7, s = 1 - (1 \times 2) = 1.$$

Thus, $x = 23, y = 6, t_2 = 5, t_1 = -7, s_2 = 2, s_1 = 1.$

When y = 6 ≠0 then

$$q = \left\lfloor \frac{23}{6} \right\rfloor = 3, r = 23 - (3 \times 6) = 5, t = 5 - (3 \times -7) = 26, s = 2 - (3 \times 1) = -1.$$

Hence, $x = 6, y = 5, t_2 = -7, t_1 = 26, s_2 = 1, s_1 = -1.$

With y =5 ≠ 0 then

$$q = \left\lfloor \frac{6}{5} \right\rfloor = 1, r = 6 - (1 \times 5) = 1, t = (-7) - (1 \times 26) = -33, s = 1 - (1 \times -1) = 2.$$

Hence, $x = 5, y = 1, t_2 = 26, t_1 = -33, s_2 = -1, s_1 = 2.$

With y = 1≠0 then

$$q = \left\lfloor \frac{5}{1} \right\rfloor = 5, r = 5 - 5 = 0, t = 26 - (5 \times -33) = 191, s = -1 - (5 \times 2) = -11.$$

Thus, 1 = gcd(191,81).

Also, $r = \{29, 23, 6, 5, 1, 0\}, t = \{-2, 5, -7, 26, -33, 191\}$

and $s = \{1, 2, 1, -1, 2, -11\}$.

The EEA (2.6) can be executed with the input (h, p). On the step (2.11), the last nonzero remainder r is equal to 1. So, the integers y, t_1, s_1 on the step (2.12) satisfy $ht_1+ks_1= y$ with y = 1, therefore $ht_1 \equiv 1 (\text{mod } p)$.

In other words, $h^{-1} \equiv t_1$ (mod p). So, the inverse element mod p, h^{-1} (mod p), can be computed using the following algorithm

Algorithm 2.7.7 Computing the inversion on F_p using the EEA [34].

```
Input: Prime $p$ and $h \in [1,p-1]$
Output: $h^{-1}$ (mod $p$).
$x \leftarrow p, y \leftarrow h.$
1. $t_1 \leftarrow 1, t_2 \leftarrow 0.$
2. While y ≠ 1 do
    3.1 $q \leftarrow \left\lfloor \frac{x}{y} \right\rfloor, r \leftarrow x - qy, t \leftarrow t_2 - qt_1.$
    3.2 $x \leftarrow y, y \leftarrow r, t_2 \leftarrow t_1, t_1 \leftarrow t.$
4. End while
5. Return ($t_1$ mod $p$).
```

Example 2.7.8 Let h =89 and p = 105 Computing 89^{-1} (mod p) can be done by using algorithm (2.4.6) as follows.

Suppose $h = y = 89$, $p = x = 105$ and the initial values are $t_1 \leftarrow 1, t_2 \leftarrow 0.$ When y = 89 ≠ 0 then

$$q = \left\lfloor \frac{105}{89} \right\rfloor = 1, r = 105 - 89 \times 1 = 16, t = 0 - 1 \times 1 = -1.$$

So, $x = 89, y = 16, t_2 = 1, t_1 = -1.$

Now, y = 16 ≠ 0 then

$$q = \left\lfloor \frac{89}{16} \right\rfloor = 5, r = 89 - 16 \times 5 = 9, t = 1 - (5 \times -1) = 6.$$

Therefore, $x = 16, y = 9, t_2 = -1, t_1 = 6.$

When $y = 9 \neq 0$ then

$q = \left\lfloor \frac{16}{9} \right\rfloor = 1, r = 16 - 9 \times 1 = 7, t = -1 - (1 \times 6) = -7.$

Hence, $x = 9, y = 7, t_2 = 6, t_1 = -7.$

Now, y = 7≠ 0 then

$q = \left\lfloor \frac{9}{7} \right\rfloor = 1, r = 9 - 7 \times 1 = 2, t = 6 - (1 \times -7) = 13.$

Hence, $x = 7, y = 2, t_2 = -7, t_1 = 13.$

With, y = 2 ≠ 0 then

$q = \left\lfloor \frac{7}{2} \right\rfloor = 3, r = 7 - 2 \times 3 = 1, t = -7 - (3 \times 13) = -46.$

Thus, $x = 2, y = 1, t_2 = 13, t_1 = -46.$

With, y = 1 ≠ 0 then

$q = \left\lfloor \frac{2}{1} \right\rfloor = 2, r = 2 - 2 \times 1 = 0, t = 13 - (2 \times -46) = 105.$

Hence, y = 0, t_2 = -46, t_1 = 105.

2.8 The Chinese remainder theorem

The Chinese remainder theorem(CRT) discussed the solve to a system of linear congruence’s. The simplest status is a system of two congruence’s [35]

$$x \equiv a \ (\text{mod } h) \text{ and } x \equiv b \ (\text{mod } k) \tag{2.19}$$

with gcd(h, k) = 1, in this a exemplar the CRT says that there is a unique solution modulo hk [36].

Example 2.8.1 It should first look for an integer x that simultaneously which solves both of the congruence’s

$$x \equiv 2 \ (\text{mod } 6) \text{ and } x \equiv 3 \ (\text{mod } 7). \tag{2.20}$$

The first congruence tells us that $x \equiv 2 \pmod 6$, so the full set of solutions to the first congruence is the collection of integers

$$x = 2+6y,\ y \in Z. \tag{2.21}$$

Substituting (2.21) into the second congruence in (2.20) gives

$$2+6y \equiv 3 \pmod 7, \text{ and hence } 6y \equiv 8 \pmod{11}. \tag{2.22}$$

We solve for y by multiplying both sides of (2.22) by the inverse of 6 modulo 7. This inverse exists because gcd(6,7) = 1. However, in this case the modulus is so small that we find it by trial and error; thus $6 \cdot 6 = 36 \equiv 1 \pmod 7$.

Theorem 2.8.2 (Euler's Formula for pq [36]. Let p and q be distinct primes and let

$$g = \gcd(p-1, q-1). \tag{2.23}$$

Then

$a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}$ for all a satisfying $gcd(a, pq)=1$.

In particular, if p and q are odd primes, then

$a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq}$ for all a satisfying $gcd(a, pq)=1$.

Proof. By assumption we know that p does not divide a and that g divides $q-1$, so we can compute

$a^{(p-1)(q-1)/g} = a^{(p-1)(q-1)/g}$ since $(q-1)/g$ is an integer,

$\equiv 1^{(q-1)/g} \pmod p$ since $a^{p-1} \equiv 1 \pmod p$ from Fermat's little theorem,

$\equiv 1 \pmod p$ since 1 to any power is 1!

The exact same computation, reversing the roles of p and q, shows that

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod q.$$

This proves that $a^{(p-1)(q-1)/g} - 1$ is divisible by both p and by q; hence it is divisible by pq.

2.9 Cryptography

Some basics and concepts are discussed to the cryptosystems as follows.

In this section, some important definitions for cryptography are presented as follows

Definition 2.9.1 Cryptography. Is the science of secret writing with the goal of hiding the meaning of a plaintext. [28].

Definition 2.9.2 Cryptanalysis is the science and sometimes art of breaking cryptosystems. You might think that code breaking is for the intelligence community or perhaps organized crime, and should not be included in a serious classification of a scientific discipline.[28].

Definition 2.9.3 Cryptosystem. Is the transformation of plaintext into ciphertext to make it secure and protected from attackers [37].

Definition 2.9.4 Plaintext**.** The plaintext is the original message in readable form and the ciphertext is the encrypted [38].

Definition 2.9.5 Security. This means keeping information transmitted across the channel secure and protected from attacks [38].

2.10 Basic Communications Model

In Figure (2.1), users Fr (the first user) and Se (the second user) are communicating via an unsecured channel. Assuming that all communications take place in the presence of an adversary E (Eve), who aims to defeat any security services being provided to Fr and Se.

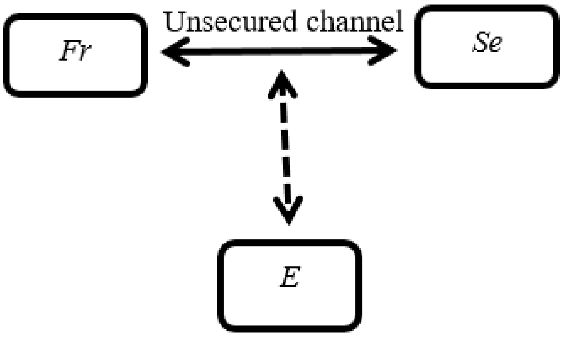


Figure 2.12. Basic communications model [27].

For example, Fr and Se could be two people communicating via a cellular telephone network, and E is attempting to wiretap on their conversation [27].

2.10.1 Asymmetric-Key Cryptographic System.

The private and public key are used to encrypt and decrypt data [29]. The keys are Unequal (asymmetric). The first is the public key can be shared in the pair with everyone, and another is a private key can stay as a secret, asymmetric encryption uses a different key for transforms plaintext into ciphertext by using a one of two keys, and using the other key to decryption, the plaintext is recovered from the ciphertext [38]. It is algorithm Diffie-Hellman, El-Gamal, RSA and Rabin. Asymmetric encryption scheme has six ingredients: plaintext, encryption algorithm, public and private keys, ciphertext, and decryption algorithm as shown in Figure (2.13) [40].

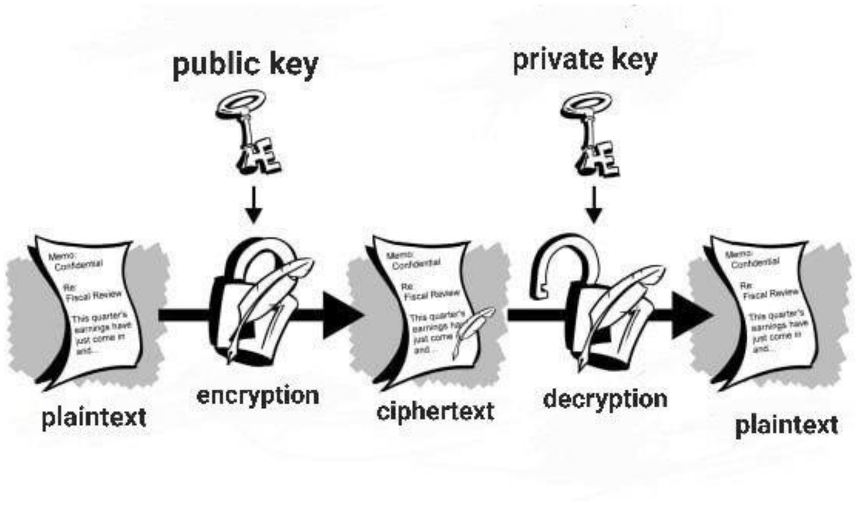


Figure 2.13. Asymmetric-Key Cryptography (Public-Key).

2.10.2 Symmetric-Key Cryptosystem

The single-key is used to encrypt and decrypt data [41]. The key is identical (symmetric). Symmetric encryption transforms plaintext into ciphertext by using a secret key (a single-key) and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext. It is four algorithms: DES, 3DES, AES, and RC4. A symmetric encryption scheme has five ingredients select plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm, as shown in Figure (2.14) [25].

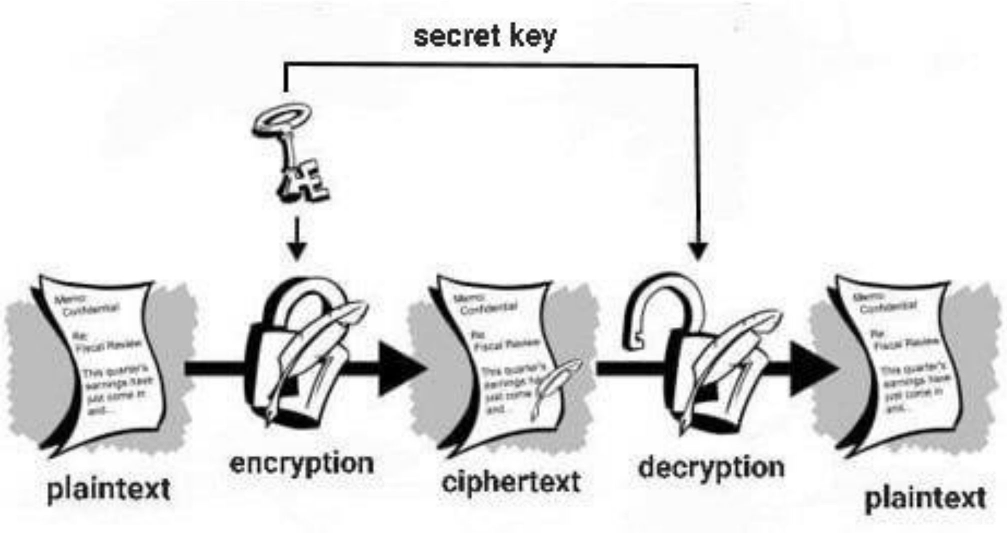


Figure 2.14. Symmetric-Key Cryptography.

2.11 Algorithms of asymmetric(public) key Cryptographic System

In this section, the original asymmetric(public) key cryptosystems are discussed as follows.

2.11.1 El-Gamal Public Key Cryptosystem.

In 1984, T. El-Gamal proposed a public-key scheme; in this section, It is described the version of El-Gamal's public-key cryptography (EPKC) that is based on the DLP that is given in Definition (2.6.1) for F_p^*. The first user starts to publish information consisting of a public key and an algorithm. The public key is a number, and the algorithm is the method by which the second user encrypts her/his plaintext using the first user's public key [42]. The first user does not disclose her/his private key, which is another number. The private key allows the first user to decrypt ciphertext that has been encrypted using her/his public key. This is all somewhat ambiguous and applies to any public-key cryptosystem. First user selects randomly an integer *a* form the range [2, *p* - 1] as her/his private key. She/He computes her/his public key Pk_A as follows [43]

$$Pk_A \equiv g^a \text{ (mod } p). \qquad (2.24)$$

Second user wants to encrypt her/his plaintext *M* and send it to first user. So, she/he randomly selects $M \in [2,p\text{-}1]$. Also, anephemeral secret key *k* is chosen, where $k \in [2,\text{p-1}]$. The ciphertext $C = (C_1, C_2)$ of *M* is computed as follows

$$C_1 \equiv g^k \ (mod\ \ p) \ \text{ and } \ C_2 \equiv M\ (Pk_A^k)(\text{mod}\, p) \qquad (2.25)$$

finally, she/he will send pair of the ciphertext (C_1, C_2) to first user. The ciphertext in the EPKC can be represented as the scheme as shown in Figure (2.15).

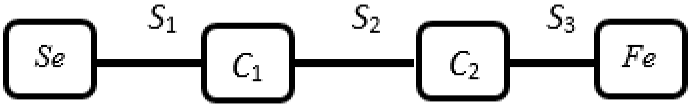


Figure 2.15. Path of encrypted plaintext EPKC.

The scheme includes one path, it contains the C_1 and C_2 of *M*. Using PTM to find the reliability of the system. The minimal path of the system is $\{S_1, S_2, S_3\}$, thus our system can be the series system, so the reliability *R* of the system as given in Equation (2.2). First user receiving the ciphertext (C_1, C_2), Several steps are calculated to restore the original plaintext *M*. She/He first computes the value *x* as following

$$x \equiv C_1^a \text{ (mod } p) \qquad (2.26)$$

Also, she/he computes the inverse value $x^{-1}(\bmod p)$ of *x*. The extended Euclidean algorithm EEA can be used to calculate the inverse number modulo *p*.

Eventually, she computes the relation

$$x^{-1} \times C_2 \equiv M \ (\text{mod } p) \qquad (2.27)$$

to recover a plaintext *M*.

Example 2.11.1.1 Let *p* = 53 be a prime number. The generator element first user selects her/his private key *a* = 15. She/He computes her/his public key Pk_A as follows

$$Pk_A \equiv g^a \ (mod\ \ p) \equiv 19^{15} \ (mod\ \ 53) \equiv 18 \ (mod\ \ 53).$$

Second user selects the plaintext $M = 44 \in [2,52]$. She/He selects an integer $k = 31 \in [1,52]$. the ciphertext computes as follows

$$C_1 \equiv g^k \ (mod\ \ p) \equiv 19^{31} \ (mod\ \ 53) \equiv 8 \ (mod\ \ 53)$$

and

$$C_2 \equiv M \ (Pk_A)^k (\text{mod}\, p) \equiv 44 \times (18)^{31} (\text{mod}\, 53) \equiv 2 (\text{mod}\, 53).$$

So, a pair of the ciphertext is $(C_1, C_2) = (8,2)$ that will be send to first user The ciphertext in the EPKC can be represented as the scheme as shown in Figure (2.16).

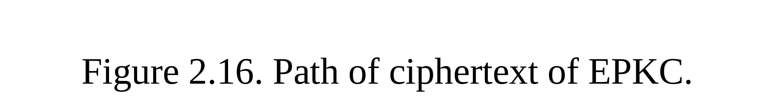


Figure 2.16. Path of ciphertext of EPKC.

The scheme includes one path, it contains the C_1 and C_2 of *M*. Using PTM to find the reliability of the system. The minimal path of the system is {S_1, S_2, S_3}, thus our system can be the series system, so the reliability *R* of the system as given in Equation (2.2).

$$R_s = R_1 R_2 R_3 .$$

First user, receives the ciphertext (8, 2), so she/he wants to decrypt it and recover the plaintext *M* through calculation as follows

$$M \equiv (C_1^a)^{-1} C_2 (modp) \equiv (8^{15})^{-1} \times 2(mod\, 53) \equiv 44(mod\, 53).$$

2.11.2 The RSA Public Key Cryptographic System.

First and second users have the usual problems of exchanging secret information via an unsafe communication channel. In this section, the RSA public key cryptosystem is described, RSA is abbreviation of the names of inventors, Rivest, Shamir, and Adleman [44].

The domain parameters of RSA cryptosystem are: *p*, *q* be large secret primes and *e* is a public encryption exponent with the property that gcd(*e*, (*p*-1)(*q*-1))=1, is selected by first user. She/ He computes her/his public modulo *N* and compute Ø(*N*), namely *N*= *pq*. So, Ø(*N*) = (*p*-1)(*q*-1). First user sent (*N*, *e*) as a public key to second user [45].

Second user wants to encrypt her/his plaintext *M* and sends it to first user. She/He first chooses her/his plaintext *M* ∈[1, *N*-1]. She/He uses first user's public key (*N*, *e*) to compute the ciphertext *C* of *M*, the ciphertext is computed as followes

$$C \equiv M^e (\text{mod} N). \qquad (2.28)$$

The ciphertext is *C* has been sent to first user. The ciphertext in the RSA can be represented as the scheme as shown in Figure (2.17).

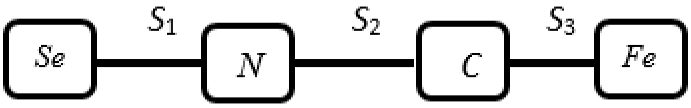


Figure 2.17. Path of encrypted plaintext of RSA.

The scheme includes one path, it contains the *N* and *C* of *M*. Using PTM to find the reliability of the system. The minimal path of the system is $\{S_1, S_2, S_3\}$, thus our system can be the series system, so the reliability R of the system as given in Equation (2.2). First user knows Ø(*N*) = (*p*-1)(*q*-1) so, used 2.29 to computed *d*

$$d \equiv e^{-1}(\mathrm{mod}(\text{Ø}(N)) \qquad (2.29)$$

First user also calculates

$$M \equiv (C^{d}(\mathrm{mod} N) \qquad (2.30)$$

Example 2.11.2.1 First user selects *p*=43, *q*=17 as secret prime numbers. The parameter *e* = 61 is selected also as a public encryption exponent with the property that gcd(*e*, (*p*-1)(*q*-1))=1. She/He computes her/his public modulo *N*. Computing Ø(*N*) is done with *N*= *pq*= 43×17 =731 so, the values of Ø(*N*) = (*p*-1)(*q*-1) =42×16 = 672.The public key of the first user is (*N*, *e*) = (731,61).

Second user wants to encrypt her/his plaintext *M*. First select *M* = 105, such that *M* ∈ [1, *N*-1]. Second user uses a public key (*N*, *e*) to compute the ciphertext *C* of *M*, it is computed as followes

$$C \equiv M^{e}(\mathrm{mod} N) \equiv (105)^{61}(\mathrm{mod} 731) \equiv 607(\mathrm{mod} 731).$$

So, the ciphertext is *C* = 607 is sent to first user. The ciphertext in the RSA can be represented as the scheme as shown in Figure (2.18).

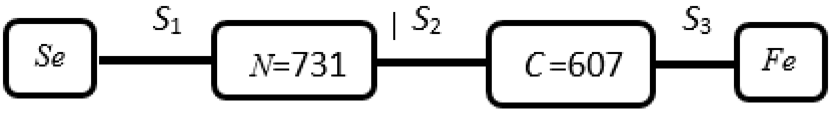


Figure 2.18. Path of ciphertext of RSA.

The scheme includes one path, it contains the *N* and *C* of *M*. Using PTM to find the reliability of the system. The minimal path of the system is $\{S_1, S_2, S_3\}$, thus our system can be the series system, so the reliability *R* of the system as given in equation (2.2)

$$R_s = R_1 R_2 R_3$$

Upon first user receives the ciphertext *C*, she/he does the following computations: Ø(*N*) = 672. So, she/he computes

$$d \equiv e^{-1} \bmod(\varnothing(N)) \equiv (61)^{-1} \bmod(731) \equiv 661 \bmod(731).$$

She/ He calculates

$$M \equiv C^{d} (\bmod N) \equiv (607)^{61} (\bmod 731) \equiv 105 (\bmod 731).$$

2.11.3 The Rabin Public Key Cryptographic System.

This section Rabin Cryptosystem(RPKC) which is computationally secure against a chosen-plaintext attack, the domain parameters for (RPKC) are: *p, q* be large secret primes. where *p, q* ≡ 3 (mod 4) and $p \neq q$ [46].

p, q: are selected by first user, She/ He computes her/his public modulus *n* where, *n*= *pq,* First user keeps the private key *p*, *q* and sends the public key *n* to second user [30].

Second user has public key *n* and her/his plaintext $M \in F_n^*$ She/He computes her/his ciphertext *C* by squaring her/his message *M* modulo *n* the ciphertext *C* of ***M*.** The ciphertext in the RPKC can be represented as the scheme as shown in Figure (2.19).

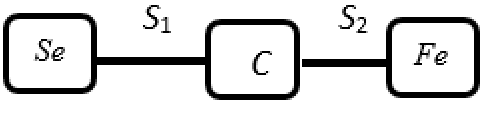


Figure 2.19. Path of encrypted plaintext of RPKC.

The scheme includes one path, it contains the *C* of *M*. Using PTM to find the reliability of the system. The minimal path of the system is {S_1, S_2, S_3}, thus our system can be the series system, so the reliability *R* of the system as given in Equation (2.2).

First user wants decryption ciphtext, she/he knows the prime factors p, q of n, She/he can make use of the fact that determining M, is equivalent to solving the following two congruence's for the values Mp and Mq

$$(Mp)^2 \equiv C(\text{mod}\, p) \text{ and } (Mq)^2 \equiv C(\text{mod} q). \qquad (2.31)$$

She/He can use Euler's criterion to determine if C is a quadratic residue modulo p (and modulo q). When $p \equiv 3 \pmod 4$, there is a simple formula to compute square roots of quadratic residues modulo p. Suppose C is a quadratic residue modulo p, where $p \equiv 3 \pmod 4$. Then we have that

$$\left.\begin{aligned} \left(\pm C^{\,(p+1)/4}\right)^2 &\equiv C^{\,(p+1)/2}\ (mod\ p) \\ &\equiv C^{\,(p-1)/2}C\ (mod\ p) \\ &\equiv C\ (mod\ p). \end{aligned}\right\} \qquad (2.32)$$

She/he use of Euler's criterion, which says that if C is a quadratic residue modulo p, then $C^{\,(p-1)/2} \equiv 1 \pmod p$. Hence, the two square roots of C modulo p are $a = \pm C^{\,(p+1)/4} \bmod p$. In a similar fashion, the two square roots of C modulo q are $b = \pm C^{\,(q+1)/4} \bmod q$, where M has $(+a, +b)$, $(+a, -b)$, $(-a, +b)$, $(-a, -b)$, by using the Chinese remainder theorem solve the congruence's [18].

Example 2.11.3.1 First user selects her/his $(p, q) = (19,7)$, be a secret prime numbers, where $p, q = (19,7) \equiv 3 \pmod 4$ and $p \neq q$, She/He compute her/his public modulus n. Where, $n = pq = 19\times7 = 133$, First user sent the publish $n = 133$ to Second user.

Second user has public key n and her/his plaintext $M = 88 \in F_{133}^{*}$. She/He computes her/his ciphertext C by squaring her/his message $M = 88$, modulo 133, the ciphertext C

$$C \equiv M^{\,2}(\text{mod}\, n) \equiv (88)^2(\text{mod}133) \equiv 30(\text{mod}133)$$

The ciphertext in the RPKC can be represented as the scheme as shown in Figure (2.20).

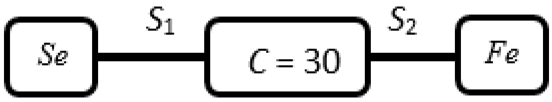


Figure 2.20. Path of ciphertext of RPKC.

The scheme includes one path, it contains the *C* of *M*. Using PTM to find the reliability of the system. The minimal path of the system is {S_1, S_2}, thus our system can be the series system, so the reliability *R* of the system as given in Equation (2.2).

$$R_s = R_1 R_2$$

First user wants decryption ciphertext, she/he knows the prime factors *p*, *q* of *n*, She/he can make use of the fact that determining *M*, is equivalent to solving the following two congruence's for the values *Mp* and *Mq*,

$$(Mp)^2 \equiv C(\bmod p) \text{ and } (Mq)^2 \equiv C(\bmod q).$$

She/He use a simple formula to compute square roots of quadratic residues modulo *p* and modulo *q* of *M*

$$a \equiv \pm C^{(p+1)/4}(\bmod p) \equiv \pm(30)^{19+1/4}(\bmod 19) \equiv \pm(30)^5(\bmod 19)$$

and

$$b \equiv \pm C^{(q+1)/4}(\bmod q) \equiv \pm(30)^{7+1/4}(\bmod 7) \equiv \pm(30)^2(\bmod 7)$$

then

$$a_1 \equiv +(30)^5(\bmod 19) \equiv 7(\bmod 19)$$
$$a_2 \equiv -(30)^5(\bmod 19) \equiv 12(\bmod 19)$$

and

$$b_1 \equiv +(30)^2 (\bmod 7) \equiv 4 (\bmod 7)$$
$$b_2 \equiv -(30)^2 (\bmod 7) \equiv 3 (\bmod 7).$$

M has four roots (a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2) = (7, 4), (7, 3), (12, 4), (12, 3) respectively by using the roots we gets the congruence's

$$\begin{aligned}
&M_{a_1b_1} \to x \equiv 7(\bmod 19), \text{ and } x \equiv 4(\bmod 7),\\
&M_{a_1b_2} \to x \equiv 7(\bmod 19), \text{ and } x \equiv 3(\bmod 7),\\
&M_{a_2b_1} \to x \equiv 12(\bmod 19), \text{ and } x \equiv 4(\bmod 7),\\
&M_{a_2b_2} \to x \equiv 12(\bmod 19), \text{ and } x \equiv 3(\bmod 7).
\end{aligned}$$

by using the Chinese remainder theorem solve the congruence's.

For *M*

$$\begin{aligned}
&M_{a_1b_1}:\\
&x = 4 + 7y\\
&4 + 7y \equiv 7(\bmod 19)\\
&7y \equiv 3(\bmod 19) \qquad ,\\
&y \equiv 14(\bmod 19)\\
&\to x = 4 + 7 \times 14\\
&x = 102
\end{aligned}$$

$$\begin{aligned}
&M_{a_1b_2}:\\
&x = 3 + 7y\\
&3 + 7y \equiv 7(\bmod 19)\\
&7y \equiv 4(\bmod 19)\\
&y \equiv 6(\bmod 19)\\
&\to x = 3 + 7 \times 6\\
&x = 45,
\end{aligned}$$

$M_{a_2b_1}:$

$x = 4 + 7y$

$4 + 7y \equiv 12(\mathrm{mod}19)$

$7y \equiv 8(\mathrm{mod}19)$,

$y \equiv 12(\mathrm{mod}19)$

$\rightarrow x = 4 + 7 \times 12$

$x = 88, \rightarrow M$

$M_{a_2b_2}:$

$x = 3 + 7y$

$3 + 7y \equiv 12(\mathrm{mod}19)$

$7y \equiv 9(\mathrm{mod}19)$

$y \equiv 4(\mathrm{mod}19)$

$\rightarrow x = 3 + 7 \times 4$

$x = 31.$

Chapter Three

Reliability
With
Path Tracing Method
for Some Kinds of Public
Key Cryptosystems

Reliability with Path Tracing Method for Some Kinds of Public Key Cryptosystems

3.1 Introduction

Asymmetric cryptosystems adopt one public key for the encryption algorithm and also one private key in the decryption algorithm. In this chapter, the use of two public keys for the encryption algorithm and two private keys in the decryption algorithm has been discussed. After dividing the plaintext into two parts in the algorithm of El-Gamal, RSA and Rabin. It is also proved on *n*-dimension.

Examples have been given to explain these reliable encryption systems. The reliability of the proposed encryption schemes was calculated based on some reliability methods, and the reduction method was also used to recover the original plaintext. A new version of asymmetric encryption algorithms has been released: R-EPKC, R-RSA and R-RPKC in the two and *n*-dimension. This version incorporates innovative techniques to ensure confidentiality and integrity of the transmitted data. With its robust design, the R-EPKC, R-RSA and R-RPKC in 2-dimension and *n*-dimension offers a more secure and efficient solution for cryptographic applications.

3.2 Reliable Public Key Cryptosystems with 2-Dimension

The Reliable El-Gamal, Reliable RSA and Reliable Rabin are encryption scheme in 2-dimensions is an improved version of the El-Gamal, RSA and Rabin encryption scheme. It provides enhanced security and reliability in the algorithms of encryption and decryption.

3.2.1 The Reliable EL-Gamal Public Key Cryptosystem.

This section proposes the 2-diminsion of the El-Gamal public key cryptosystem (R-EPKC) the domain parameters for 2D-REPKC are: a prime *p* and a generator element g in a prime field F_p, a private key $a = (a_1, a_2)$ is selected by first user. She/ He computes her/his public key

$$Pk_A = (PK_{A_1}, PK_{A_2})$$

by

$$PK_{A_1} \equiv g^{a_1} (\bmod p) \text{ and } PK_{A_2} \equiv g^{a_2} (\bmod p).$$

Second user wants to encrypt her/his plaintext M (study two cases a number and an english word) and sends to first user She/He first divided M into two parts m_1 and m_2 where $m_1,m_2 \in[2,p-1]$. An ephemeral secret keys k_1 and k_2 is chosen, where k_1, $k_2 \in[2,p-1]$. The ciphertext (C_1, C_2) and (C_1', C_2') of m_1 and m_2 is computed as follows, for a ciphertext m_1, the ciphertext is computed by

$$C_1 \equiv g^{k_1} (\bmod p) \text{ and } C_2 \equiv m_1 (PK_{A_1})^{k_1} (\bmod p).$$

While, the ciphertext of m_2 is

$$C_1' \equiv g^{k_2} (\bmod p) \text{and } C_2' \equiv m_2 (PK_{A_2})^{k_2} (\bmod p).$$

The ciphertext is ((C_1, C_2), (C_1', C_2')) has been sent to first user. The ciphertext in the R-EPKC can be represented as the network system as shown in Figure (3.21).

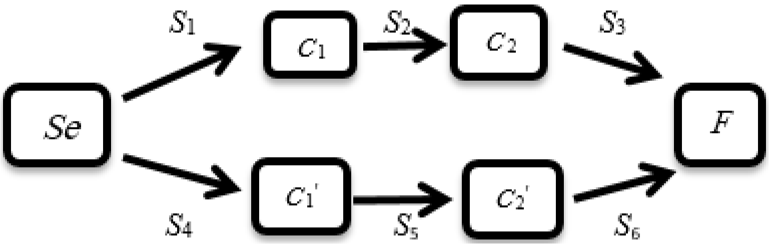


Figure 3.1. Network system of the ciphertext ((C_1, C_2), (C_1', C_2')) in the R-EPKC.

The R-EPKC consists of two paths, the first one contains the C_1 and C_2 of m_1 and the second one contains $C_1^{'}$ and $C_2^{'}$ of m_2. The reliability of the proposed R-EPKC can be determined using PTM as discussed in Section (2. 3.1) of Chapter (2). The minimal path sets of proposed cryptosystem are $\{S_1, S_2, S_3\}$and $\{S_4, S_5, S_6\}$. Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.2).

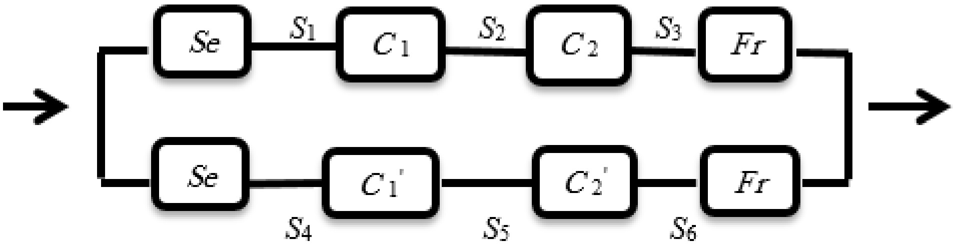


Figure 3.2. A parallel-series system of R-EPKC.

The paths for this system, in Figure (3.2), are: $P_1= S_1S_2S_3$ and $P_2 = S_4S_5S_6$. The reliability Rs_j with j = 1,2 of series paths computes based on the reliability R_i of subsystems S_i for i = 1,2,3,4,5,6. So, the reliability is computed by

$$Rs_j = \prod_{i=1}^{n} R_i \text{, where } n \text{ is the number of subsystems } S_i \text{ in path } P_j. \qquad (3.33)$$

Based on Figure (3.22), the reliability of parallel system R_S is determined by

$$Rs = 1 - \prod_{j=1}^{m} (1 - Rs_j), \text{ where } m \text{ is the number of the paths } P_j. \qquad (3.34)$$

After first user receiving the ciphertext. She/He want to decrypt the ciphertext and recover the original plaintext. So, She/ He calculates the following steps

$$m_1 \equiv ((C_1)^{a_1})^{-1} \times C_2 (\bmod p) \text{ and } m_2 \equiv ((C_1^{'})^{a_2})^{-1} \times C_2^{'} (\bmod p).$$

The original plaintext is M = (m_1, m_2). New technique to combine encrypted messages with a reliable method that is called parallel-series reduction method (PSRM) which is employed for decrypting the ciphertext and recovering the original plaintext. Suppose the system whose a reliability is given in Figure (3.3). The system has six components and two paths.

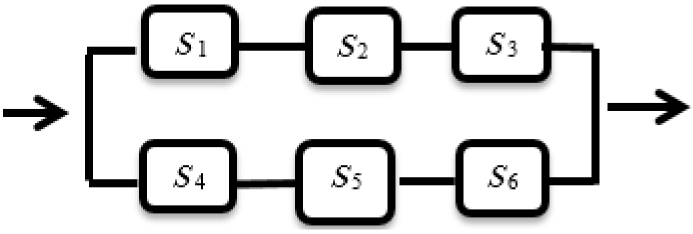


Figure 3.3. A parallel-series block diagram of the plaintext paths.

Based on the system structure given in Figure (3.3), the components S_1, S_2 and S_3 form a series subsystem that can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components $m_1=S_1S_2S_3$. Similarly, the components S_4, S_5 and S_6 form a series subsystem which is remodeled by a super-component referred to as m_2. The super-component reliability is the product of the path components $m_2=S_4S_5S_6$. The block diagram of two series reductions can be represented in given in Figure (3.3) which is transformed into Figure (3.4).

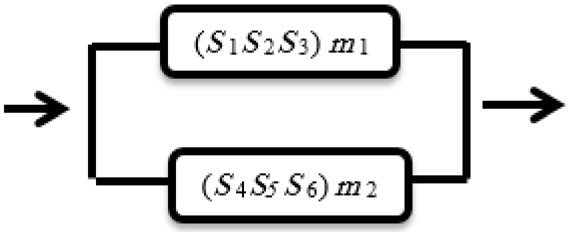


Figure 3.4. A parallel block diagram of the plaintext paths.

Based on the system structure given in Figure (3.4), the components m_1, m_2 form a parallel subsystem that is remodeled by a super-component referred to M. The reliability of super-component M as given in Equation (3.4)

The block diagram of parallel reductions in Figure (3.4) is transformed into Figure (3.5).

Figure 3.5. The original plaintext.

3.2.1.1. The Computational Results on Alternative Version REPKC

In this section, some examples are discussed of two cases of the modified R-EPKC which are taken the plaintexts as numbers (or as texts). These examples are considered as study cases that are discussed in the following section.

3.2.1.1.1. Study Case of the Plaintext as Numbers

Let p=17 be a prime number and g = 2 be a generator element in F_{17}. First user selects her/his private key by $a = (a_1, a_2) = (5, 7)$ such that $a_1, a_2 \in [2,16]$. She/He computes her/his public key

$PK_A = \left(PK_{A_1}, PK_{A_2}\right)$by

$$PK_{A_1} \equiv g^{a_1}(\bmod p) \equiv 2^5(\bmod 17) \equiv 15(\bmod 17)$$

and

$$PK_{A_2} \equiv g^{a_2}(\bmod p) \equiv 2^7(\bmod 17) \equiv 9(\bmod 17).$$

Second user wants to encrypt his/her plaintext M. He/She divided it into two parts m_1 = 7and m_2 =10. An ephemeral secret keys is chosen by $(k_1, k_2) = (6,11)$ such that k_1 and $k_2 \in [2,16]$. The ciphertext $((C_1, C_2), (C_1', C_2'))$ of (m_1, m_2) is computed for m_1, and m_2 respectively by

$$C_1 \equiv g^{k_1}(\bmod p) \equiv 2^6(\bmod 17) \equiv 13(\bmod 17)$$

and

$$C_2 \equiv m_1 Pk_{A_1}^{\ k_1}(\bmod p) \equiv 7 \times 15^6(\bmod 17) \equiv 6(\bmod 17).$$

$$C_1' \equiv g^{k_2} (\bmod\, p) \equiv 2^{11} (\bmod 17) \equiv 8 (\bmod 17)$$

and

$$C_2' \equiv m_2 Pk_{A_2}{}^{k_2} (\bmod\, p) \equiv 10 \times 9^{11} (\bmod 17) \equiv 14 (\bmod 17).$$

So, a pair of the ciphertext ((13, 6), (8, 14)) in R-EPKC can be represented as the network system as shown in Figure (3.6) and will be sent to first user.

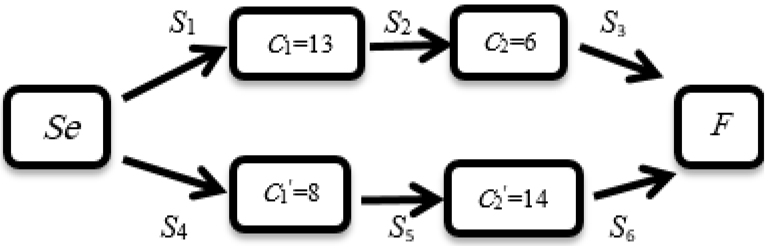


Figure 3.6. Network system of the ciphertext in the R-EPKC.

First user receives the network system diagram, she/he explains this diagram as follows. The R-EPKC consists of two paths, the first path contains the C_1 and C_2 of m_1 and the second path contains C_1' and C_2' of m_2. The reliability of the proposed 2D-EPKC can be determined using PTM as explained in Section (2.3.1). The minimal path sets of proposed cryptosystem are $\{S_1, S_2, S_3\}$ and $\{S_4, S_5, S_6\}$. Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.7).

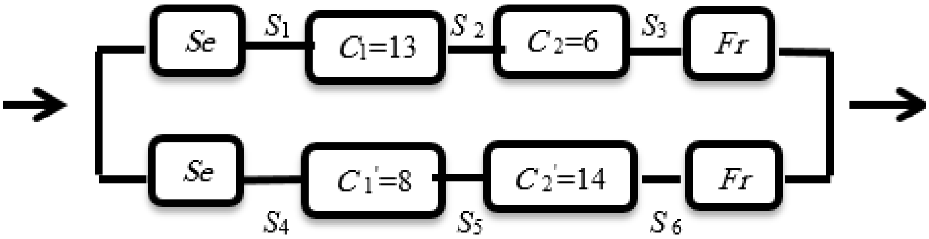


Figure 3.7. A parallel-series system of the ciphertext ((13,6), (8,14)) in R-EPKC.

The paths for this system, in Figure (3.7) are: $P_1 = S_1S_2S_3$ and $P_2 = S_4S_5S_6$. The reliability Rs_j with j = 1,2 of series paths computes based on the reliability R_i of subsystems S_i for i=1,2,3,4,5,6. So, the reliability is computed as given in Equation (3.33). Based on Figure (3.7), one can compute

$$Rs_1 = R_1R_2R_3 \text{ and } Rs_2 = R_4R_5R_6.$$

The reliability of parallel system R_S is determined as given in Equation (3.34). The reliability of system is computed by

$$\begin{aligned} R_{s_j} &= 1-[(1-R_{s_1})\ (1\text{-}\mathrm{R}_{s_2})] \\ &= 1-[(1-R_1R_2R_3)(1-R_4R_5R_6)] \\ &= R_4R_5R_6 + R_1R_2R_3 - R_1R_2R_3R_4R_5R_6. \end{aligned}$$

First user also calculates

$$m_1 \equiv (C_1^{a_1})^{-1} \times C_2 (\mathrm{mod}\, p) \equiv (13^5)^{-1} \times 6(\mathrm{mod}17) \equiv 7(\mathrm{mod}17)$$

and

$$m_2 \equiv (C_1^{'a_2})^{-1} \times C_2' (\mathrm{mod}\, p) \equiv (8^7)^{-1} \times 14(\mathrm{mod}17) \equiv 10(\mathrm{mod}17).$$

The original plaintext is $M = (m_1, m_2) = (7,10)$.

New technique to combine encrypted messages with a reliable method that is called parallel-series reduction method (PSRM) is proposed in this work and which is employed for decrypting the ciphertext and recovering the original plaintext. The cryptosystem in Figure (3.7) has been represented by two paths as shown in Figure (3.8).

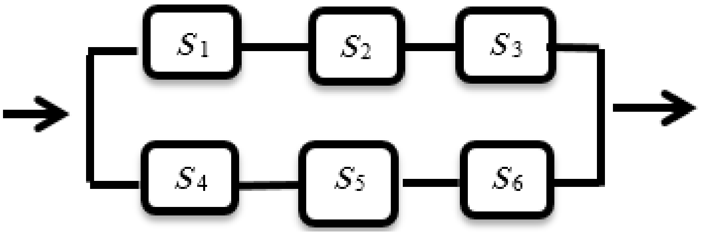


Figure 3.8. Two paths of plaintext M = (7,10).

Based on the system structure given in Figure (3.8), the components S_1, S_2 and S_3 create a series subsystem which can be remodeled by the super-component that is referred to m_1. Super-component reliability is the product of the path components $m_1 = R_1R_2R_3$. In similar way, the components S_4, S_5 and S_6 form a series subsystem that can be remodeled by a super-component which is referred to m_2. The super-component reliability here is determined by the product of the path components $m_2 = R_4R_5R_6$. The block diagram of two series reductions in Figure (3.8) is transformed into Figure (3.9).

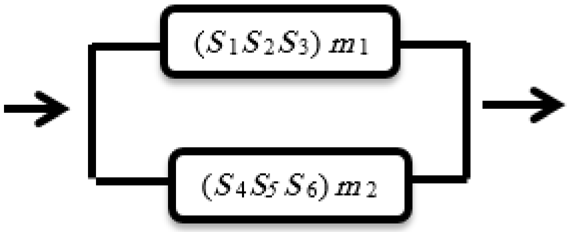


Figure 3.9. A parallel block diagram of the plaintext paths M = (7,10).

Using the system structure given in Figure (3.9), the reliability of super-component $M = (m_1, m_2)$ is computed by

$$R_m = 1-(1-R_{m_1})(1-R_{m_2}) = R_{m_1} + R_{m_2} - R_{m_1}R_{m_2}.$$

The block diagram of parallel reductions in Figure (3.9) is transformed into Figure (3.10).

Figure 3.10. The path of the original plaintext M = (7,10).

Other computational results with various values of prime numbers p is presented in Table (3.1).

Table 3.1 Results of (2D-R-EPKC).

Input	Private key(Fr) a_1,a_2	Public key Pk_{A1} , Pk_{A2}	Private key(Se) k_1 , k_2	Encryption C_1, C_2	Decryption m_1, m_2
p =197 g=31	51	139	117	176 , 18	85
	15	124	128	132 , 98	87
p =281 g =73	108	222	115	113 ,217	279
	193	92	149	38 , 150	252
p =383 g =257	301	231	288	73 , 266	370
	373	218	315	127 , 258	299
p =683 g =367	453	418	591	138 ,606	601
	521	311	533	571 , 293	588
p =829 g =419	751	263	623	407 , 350	811
	801	317	773	40 , 20	808

3.2.1.1.2. Study Case of the Plaintext as English Word

Let p=127 be a prime number and g =11 be a generator element in F_{127}. First user selects her/his private key by (a_1, a_2) = (10, 15) such that a_1, $a_2 \in$ [2,126]. She/He computes her/his public key PK_A = $\left(PK_{A_1}, PK_{A_2}\right)$by

$$PK_{A_1} \equiv g^{a_1}(\bmod p) \equiv 11^{10}(\bmod 127) \equiv 98(\bmod 127)$$

and

$$PK_{A_2} \equiv g^{a_2}(\bmod p) \equiv 11^{15}(\bmod 127) \equiv 73(\bmod 127).$$

Second user wants to encrypt his/her plaintext M which is **IRAQ** word such that IRAQ = (m_1, m_2, m_3, m_4), that is transferred into numbers by (m_1, m_2, m_3, m_4) = (73, 82, 65, 81) using the ASCII values as shown in Table (2.1). An ephemeral secret key (k_1, k_2) = (12,17) is chosen such that k_1, $k_2 \in$ [2,126]. The ciphertext C = ((C_1, C_2), (C_1, C_3), (C_1', C_2'), (C_1', C_3')) of M. In more details, the ciphertexts of m_1 and m_2 are computed by

$$C_1 \equiv g^{k_1} (\bmod p) \equiv 11^{12} (\bmod 127) \equiv 47 (\bmod 127),$$

$$C_2 \equiv m_1 (Pk_{A_1})^{k_1} (\bmod p) \equiv 73 \times 98^{12} (\bmod 127) \equiv 32 (\bmod 127)$$

and

$$C_3 \equiv m_2 (Pk_{A_1})^{k_1} (\bmod p) \equiv 82 \times 98^{12} (\bmod 127) \equiv 69 (\bmod 127).$$

While, the ciphertexts of m_3 and m_4 are

$$C_1^{'} \equiv g^{k_2} (\bmod p) \equiv 11^{17} (\bmod 127) \equiv 70 (\bmod 127),$$

$$C_2^{'} \equiv m_3 (Pk_{A_2})^{k_2} (\bmod p) \equiv 65 \times 73^{17} (\bmod 127) \equiv 28 (\bmod 127)$$

and

$$C_3^{'} \equiv m_4 (Pk_{A_2})^{k_2} (\bmod p) \equiv 81 \times 73^{17} (\bmod 127) \equiv 115 (\bmod 127).$$

So, the pairs of the ciphertexts $((C_1, C_2), (C_1, C_3), (C_1^{'}, C_2^{'}), (C_1', C_3'))$ is represented by the network system as shown in Figure (3.11) and sent to first user.

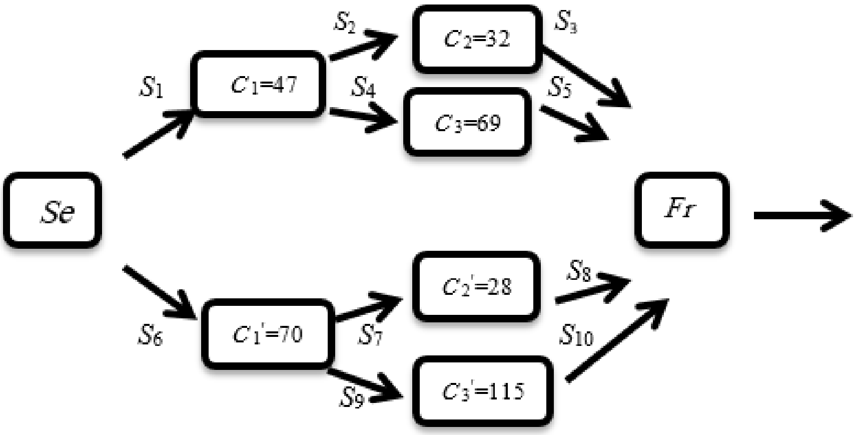


Figure 3.11. Network system of the ciphertext

((47,32), (47,69), (70,28), (70,115)) in the R-EPKC.

The R-EPKC consists of four paths, the first one contains the C_1 and C_2 of m_1, the second one contains C_1 and C_3 of m_2, the third one path contains $C_1^{'}$ and $C_2^{'}$ of m_3 and four path contains $C_1^{'}$ and $C_3^{'}$ of m_4. The reliability of the proposed R-EPKC can be determined using PTM. The minimal path sets of proposed cryptosystem are $\{S_1, S_2, S_3\}$, $\{S_1, S_4, S_5\}$, $\{S_6, S_7, S_8\}$, $\{S_6, S_9, S_{10}\}$. Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.12)

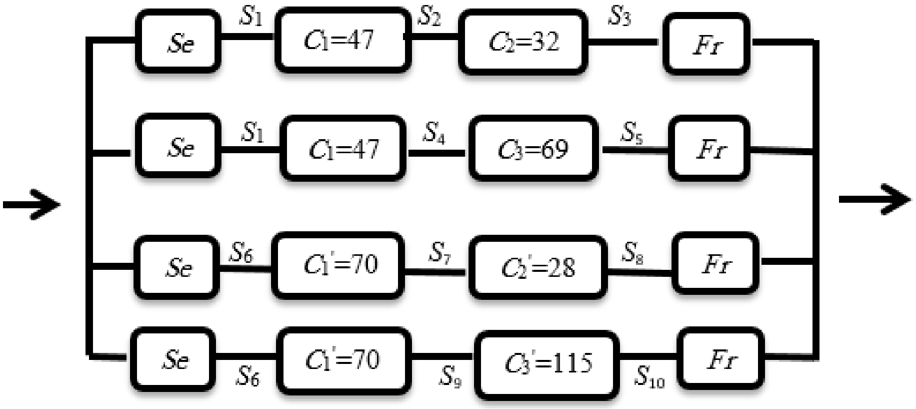


Figure 3.12. A parallel-series system of the ciphertext ((47,32), (47, 69), (70,28), (70,115)).

The paths for this system, in Figure (3.32), are: $P_1 = S_1S_2S_3$, $P_2 = S_1S_4S_5$, $P_3 = S_6S_7S_8$, $P_4 = S_6S_9S_{10}$. The reliability Rs_j with j = 1,2,3,4 of series paths computes based on the reliability R_i of subsystems S_i for i =1, …,10. So, the reliability is computed as given in Equation (3.33). Based on Figure (3.12), one can compute

$$Rs_1 = R_1R_2R_3,\ Rs_2 = R_1R_4R_5,\ Rs_3 = R_6R_7R_8 \text{ and } Rs_4 = R_6R_9R_{10}.$$

The reliability of parallel system R_S is determined as given in Equation (3.34).

The reliability of system is

$$R_s = 1-[(1-R_1R_2R_3)(1-R_1R_4R_5)(1-R_6R_7R_8)(1-R_6R_9R_{10})]$$

$$\begin{aligned}
&= R_1R_2R_3 + R_1R_4R_5 - R_1R_2R_3R_4R_5 \\
&+ R_6R_7R_8 - R_1R_4R_5R_6R_7R_8 - R_1R_2R_3R_6R_7R_8 \\
&+ R_1R_2R_3R_4R_5R_6R_7R_8 + R_6R_9R_{10} - R_6R_7R_8R_9R_{10} \\
&- R_1R_4R_5R_6R_9R_{10} - R_1R_2R_3R_6R_7R_8 + R_1R_2R_3R_4R_5R_6R_7R_8R_9R_{10}.
\end{aligned}$$

After first user receiving the ciphertext ((47,32), (47,69), (70,28), (70,115)), she/he want to decrypt the ciphertext and recover the original plaintext. So, she/he calculates the following steps

$$m_1 \equiv (C_1^{a_1})^{-1} \times C_2 (\bmod p) \equiv (47^{10})^{-1} \times 32 (\bmod 127) \equiv 73 (\bmod 127),$$

$$m_2 \equiv (C_1^{a_1})^{-1} \times C_3 (\bmod p) \equiv (47^{10})^{-1} \times 69 (\bmod 127) \equiv 82 (\bmod 127),$$

$$m_3 \equiv (C_1'^{a_2})^{-1} C_2' (\bmod p) \equiv (70^{15})^{-1} \times 28 (\bmod 127) \equiv 65 (\bmod 127)$$

and

$$m_4 \equiv (C_1'^{a_2})^{-1} C_3' (\bmod p) \equiv (70^{15})^{-1} \times 115 (\bmod 127) \equiv 81 (\bmod 127).$$

The original plaintext (m_1, m_2, m_3, m_4) = (73, 82, 65, 81). The PSRM is used to combine encrypted messages with a reliable method. This method is employed for decrypting the ciphertext and recovering original plaintext.

The cryptosystem in Figure (3.12) has been represented by four paths as shown in Figure (3.13).

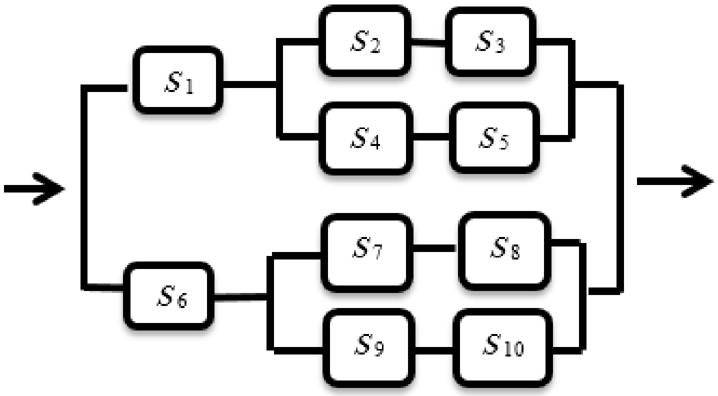
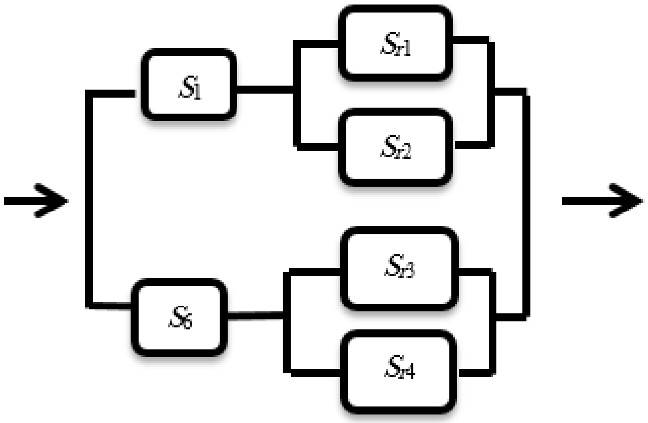


Figure 3.13. Mixed system of the plaintext paths.

Based on the system structure given in Figure (3.13), the components S_2, S_3 create a series subsystem which can be remodeled by a super-componentthat is referred to as S_{r1}, super-component reliability is the product of the path components $R_{r1} = R_2R_3$. In similarty the components S_4, S_5 from a series subsystem that can be remodeled by a super-component which is referred to S_{r2}, and a super-component reliability is the product of the path components $R_{r2} = R_4R_5$, the components S_7, S_8 from a series subsystem, which can be remodeled by a super-component referred to as S_{r3}, and super-component reliability is the product of the path components $R_{r3} = R_7R_8$, and the components S_9, S_{10} from a series subsystem, which can be remodeled by a super-component referred to as S_{r4}, and super-component reliability is the product of the path components $R_{r4} = R_9R_{10}$. The block diagram of the four series reductions, in Figure (3.13) is transformed into Figure (3.14).



Figuer 3.14. Mixed system after serise reduction plaintext paths

Based on the system structure given in Figure (3.14), the components S_{r1} and S_{r2}, form a parallel subsystem, which can be remodeled by a super-component referred to as S_{r5}. The reliability of super-component S_{r5} computed by

$$\begin{aligned} R_{r_5} &= 1-(1-R_{r_1})(1-R_{r_2}) \\ &= 1-(1-R_2R_3)(1-R_4R_5) \\ &= R_2R_3+R_4R_5-R_2R_3R_4R_5. \end{aligned}$$

and the components S_{r3} and S_{r4} form a parallel subsystem, which can be remodeled by a supercomponent referred to as S_{r6}. The reliability of supercomponent S_{r6} computed by

$$\begin{aligned} R_{r_6} &= 1-(1-R_{r_3})(1-R_{r_4}) \\ &= 1-(1-R_7R_8)(1-R_9R_{10}) \\ &= R_7R_8+R_9R_{10}-R_7R_8R_9R_{10}. \end{aligned}$$

The block diagram of two parallel reductions in Figure (3.14) is transformed into Figure (3.15).

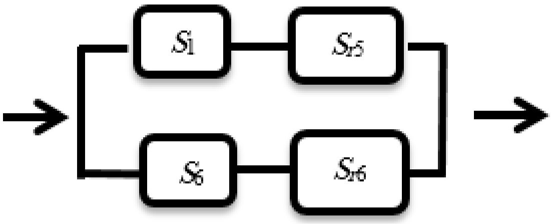


Figure 3.15. The system of the plaintext after parallel reduction.

The components S_1 and S_{r5} form a series subsystem which can be remodeled by a super-component referred to S_{r7}. The super-component reliability is the product of the path components $R_{r7} = R_1R_{r5}$, In similarty the components S_6 and S_{r6} form a series subsystem, which can be remodeled by a super-component referred to as S_{r8}. the super-component reliability is the product of the path components $R_{r8} = R_6R_{r6}$. The block diagram of two series reductions in Figure (3.15) is transformed into Figure (3.16).

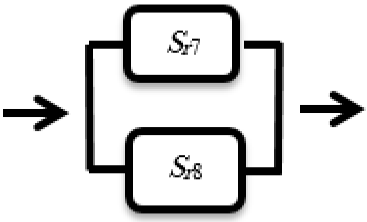


Figure 3.16. The plaintext paths after 2 serise reduction.

And the components S_{r7} and S_{r8}, from a parallel subsystem, which can be remodeled by a super-component referred to S_{r9}. The reliability of super-component S_{r9} is

$$\begin{aligned} R_{r_9} &= 1-(1-R_{r_7})(1-R_{r_8}) \\ &= R_{r_7} + R_{r_8} - R_{r_7} R_{r_8}. \end{aligned}$$

the block diagram of parallel reductions in Figure (3.16) is transformed into Figure (3.17)

Figure 3.17. The original plaintext M = (73, 82, 65, 81).

The original plaintext is M = (73, 82, 65, 81). Using the ASCII values, M can be converted easily by (73, 82, 65, 81) which is corresponded to **IRAQ**.

3.2.2 The Reliable RSA Public Key Cryptosystem.

This section proposes the 2-diminsion of the RSA public key cryptosystem which is called reliable (R-RSA) cryptosystem. The domain parameters of R-RSA are: p_1, p_2, q_1 and q_2 are large secret primes, and e a public encryption exponent with the property that gcd (e, (p_i-1)(q_i-1)) = 1, i = 1, 2 which are selected by first user. She/He computes her/his public modulus N_i and compute Ø(N_i), with i =1, 2 namely $N_1 = p_1q_2$, $N_2 = p_2q_2$ and Ø(N_1) = (p_1-1)(q_1-1), Ø(N_2) = (p_2-1)(q_2-1), First user sent the public key (N_1, N_2, e) to second user. Second user wants to encrypt his/her plaintext M. He/She first chooses his/her plaintext M and divides it into two parts m_1 and m_2, where $m_1 \in [1, N_1-1]$, $m_2 \in [1, N_2-1]$. He/She uses first user's public key (N_1, N_2, e) to compute the ciphertext C_1 and C_2 of m_1 and m_2 respectively by

$$C_1 \equiv m_1^e \pmod{N_1} \text{ and } C_2 \equiv m_2^e \pmod{N_2}.$$

The ciphertext is C_1 and C_2 has been sent to first user as the network cryptosystem of the ciphertext (C_1, C_2) and public parameters N_1 and N_2, shown in Figure (3.18).

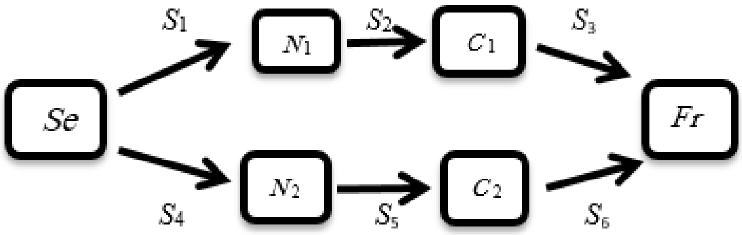


Figure 3.18. Network system of the (C_1, C_2), N_1 and N_2 in the R-RSA.

First user after receiving the network cryptosystem, he/she discusses the ciphertext in Figure (3.38) as follows. The R-RSA consists of two paths, the first path contains the N_1 and C_1 of m_1 and the second path contains N_2 and C_2 of m_2. The reliability of the proposed R-RSA can be determined using PTM. The minimal path sets of proposed cryptosystem are $\{S_1, S_2, S_3\}$and $\{S_4, S_5, S_6\}$. Thus, the proposed cryptosystem can be represented as the series-parallel system as shown in Figure (3.19).

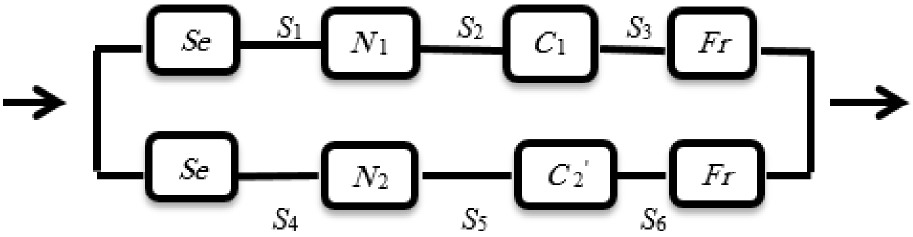


Figure 3.19. A parallel-series system of the ciphertext in the R-RSA.

The paths for this system, in Figure (3.19), are: P_1= $S_1S_2S_3$ and P_2 = $S_4S_5S_6$. The reliability Rs_j with j=1,2 of series paths computes based on the reliability R_i of subsystems S_i for i =1, …,6. So, the reliability is computed as given in Equation (3.33). The reliability of parallel system R_S is determined as given in Equation (3.34). First user knows $Ø(N_1)$ = $(p_1$-1)(q_1-1) and $Ø(N_2)$ = (p_2-1)(q_2-1), so $ed_i \equiv$ 1mod(p_i-1)(q_i-1) for i = 1,2 can be solved, to determine the values of

$$d_1 \equiv e^{-1} \text{mod}(Ø(N_1)) \text{ and } d_2 \equiv e^{-1} \text{mod}(Ø(N_2)).$$

Upon first user receives the ciphertext, she/he wants to decrypt the ciphertext and recover the original plaintext. So, she/he calculates m_1 and m_2 by

$$m_1 \equiv (C_1^{d_1}(\mathrm{mod}\, N_1) \text{ and } m_2 \equiv C_2^{d_2}(\mathrm{mod}\, N_2).$$

The original plaintext is M = (m_1, m_2). The P-SRM is used decrypting the ciphertext and recovering the original plaintext M. The system of the ciphertext in Figure (3.19) whose reliability given in Figure (3.20). The reliability system in Figure (3.20) has two paths with six components.

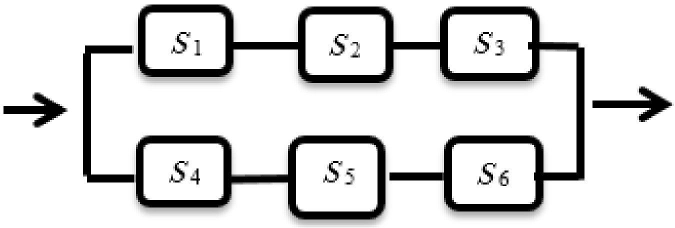


Figure 3.20. A P-SS of the plaintext.

In last Figure, the components S_1, S_2, S_3 form a series subsystem that can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components $m_1 = S_1S_2S_3$. Similarly, the components S_4, S_5, S_6 form a series subsystem which can be remodeled by a super-component referred to m_2. The super-component reliability is the product of the path components $m_2 = S_4S_5S_6$. The block diagram of two series reductions in Figure (3.20) has been transformed into Figure (3.21).

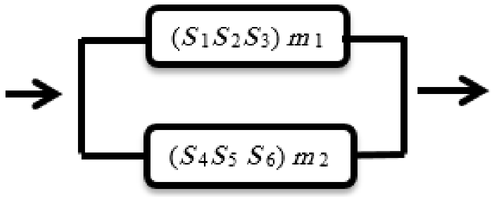


Figure 3.21. Block diagram of the plaintext after two reduction.

In Figure (3.21), the components m_1 and m_2 form a parallel subsystem which can be remodeled by a super-component referred to M. The reliability of super-component M as given in Equation (3.34). The block diagram of the parallel reductions in Figure (3.41) is transformed into Figure (3.22).

$(S_1S_2S_3S_4S_5S_6)\ M$

Figure 3.22. The plaintext $M = (m_1, m_2)$ after parallel reduction.

3.2.2.1 The Study Case on the R-RSA Cryptosystem

First user selects her/his (p_1, = 11, $p_2 = 89$, $q_1 = 13$ and $q_2 = 5$ as the secret prime numbers. She/He selects e =71 as a public encryption exponent with the property that gcd(e, (p_i-1)(q_i-1)) =1, i = 1, 2. She/He computes her/his public modulus

$$N_1 = p_1q_2 = 11\times13 = 143 \text{ and } N_2 = p_2q_2 = 89\times5 = 445,$$

and computes

$$Ø(N_1) = (p_1\text{-}1)(q_1\text{-}1) = 10\times12 = 120,\ Ø(N_2) = (p_2\text{-}1)(q_2\text{-}1) = 88\times4 = 352.$$

The first user public key is

$$(N_1, N_2, e) = (143,445,71).$$

Sceond user wants to encrypt his/her plaintext M. He/She divided it into two parts $m_1 \in [1,142]$ and $m_2 \in [1,444]$, where $(m_1, m_2) = (43,59)$. Second user uses a public key (N_1, N_2, e) to computed the ciphertext C_1 and C_2 of m_1 and m_2 respectively. For m_1, the ciphertext is computed by

$$C_1 \equiv m_1^e (\text{mod} N_1) \equiv 43^{71} (\text{mod}143) \equiv 10 (\text{mod}143).$$

While, the ciphertext of m_2 is

$$C_2 \equiv m_2^e (\text{mod} N_2) \equiv 59^{71} (\text{mod}\,445) \equiv 439 (\text{mod}\,445).$$

The ciphertext (C_1, C_2) and parameters N_1 and N_2 in the R-RSA cryptosystem have been represented by the network system as shown in Figure (3.23).

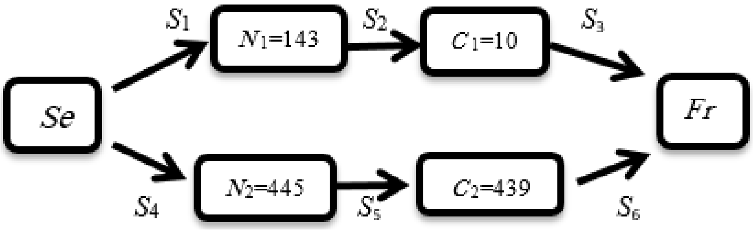


Figure 3.23. Network system of the (C_1, C_2) = (10,439),

N_1 = 143 and N_2 =445 in the R-RSA.

Two paths of the R-RSA cryptosystem are formed, first one contains the N_1 and C_1 of m_1 and second one contains N_2 and C_2 of m_2. The reliability of the proposed R-RSA can be determined using PTM. The minimal path sets of proposed cryptosystem are {S_1, S_2, S_3}and {S_4, S_5, S_6}. Thus, the proposed cryptosystem can be represented as the series-parallel system as shown in Figure (3.24).

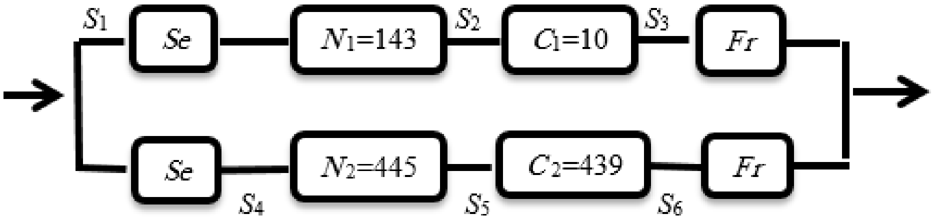


Figure 3.24. A parallel-series system of the (C_1, C_2) = (10,439),

N_1 = 143 and N_2 =445 in R-RSA cryptosystem.

The paths for this system, in Figure (3.24), are: P_1= $S_1S_2S_3$ and P_2 = $S_4S_5S_6$. The reliability Rs_j with j=1,2 of series paths computes based on the reliability R_i of subsystems S_i for i=1,2,3,4,5,6. So, the reliability is computed as given in Equation (3.33). Based on Figure (3.24), one can compute

$$Rs_1 = R_1R_2R_3 \text{ and } Rs_2 = R_4R_5R_6.$$

The reliability of parallel system R_S is determined as given in Equation (3.34).

$$\begin{aligned} R_{s_j} &= 1-[(1-R_{s_1})\ (1\text{-R}_{s_2})] \\ &= 1-[(1-R_1R_2R_3)(1-R_4R_5R_6)] \\ &= R_4R_5R_6+R_1R_2R_3-R_1R_2R_3R_4R_5R_6. \end{aligned}$$

Upon first user receives the ciphertext (C_1, C_2) = (10, 439), she/he does the following computations Ø(N_1) =120 and Ø(N_2) = 352 so, she/he computes

$$d_1 \equiv e^{-1}\,\text{mod}(\varnothing(N_1)) \equiv 71^{-1}\,\text{mod}(120) \equiv 71\text{mod}(120)$$

and

$$d_2 \equiv e^{-1}\,\text{mod}(\varnothing(N_2)) \equiv 71^{-1}\,\text{mod}(352) \equiv 119\,\text{mod}(352).$$

She/ He calculates

$$m_1 \equiv (C_1^{d_1}(\text{mod}\,N_1) \equiv 10^{71}(\text{mod}143) \equiv 43(\text{mod}143)$$

and

$$m_2 \equiv C_2^{d_2}(\text{mod}\,N_2) \equiv 439^{119}(\text{mod}\,445) \equiv 59(\text{mod}\,445).$$

The original plaintext of the M = (m_1, m_2) = (43,59). The P-SRM is employed for decrypting the ciphertext and recovering the original plaintext. The reliability system is represent as given in Figure (3.20). with six components through two paths. The components S_1, S_2, S_3 form a series subsystem that is can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components m_1= $R_1R_2R_3$. In Similar way the components S$_4$, S_5, S_6 from a series subsystem that can be remodeled by a super-component referred to m_2. The super-component reliability is the product of the path components m_2 = $R_4R_5R_6$. The block diagram of a two series reductions is represented as given in Figure (3.21). Using Figure (3.21), the components m_1 and m_2 form a parallel subsystem, which can be remodeled by a super-component referred to M the reliability of super-component M is

$$R_m = 1-(1-R_{m_1})(1-R_{m_2}) = R_{m_1} + R_{m_2} - R_{m_1}R_{m_2}.$$

The block diagram of the parallel reductions is given as in Figure (3.42).

Other computational results with various values of prime numbers *p* is presented in Table (3.2).

Table 3.2 Results of (2D-R-RSA).

Private key		Public key		Ø(*N*)	Encryption C	Decryption	
P	*Q*	N	*E*			*D*	*M*
601	557	334757	439	333600	107027	8359	661
761	647	492367		490960	32439	27959	540
977	151	147527	353	146400	121841	135617	801
863	587	506581		505132	301042	459341	593
991	199	197209	557	196020	129925	13373	691
797	277	220769		219696	79905	176309	885
809	239	193351	619	192304	29022	47843	811
829	701	581129		5796600	341791	179779	721
863	433	373679	719	372384	113658	32111	814
743	241	179063		178080	121601	92879	818

3.2.3 The Reliable Rabin Public Key Cryptosystem.

The alternative version of the Rabin public key cryptosystem. **(**RPKC) has been proposed with two dimension. It is computationally more secure in compare with the original one. On proposed RPKC which is also called reliable Rabin public key cryptosystem (R-RPKC), first user selects the parameters: p_1, p_2, q_1 and q_2 as the large secret primes, where p_1, q_1, p_2 and $q_2 \equiv 3 \pmod 4$ with $p_1 \neq q_1$, $p_2 \neq q_2$. She/He also computes her/his public modulus's $n_1 = p_1q_1$ and $n_2 = p_2q_2$. She/He keeps the private key p_1, q_1 and p_2, q_2

Second user knows the public key n_1 and n_2. The plaintext M of his/her is chosen and divided into two parts m_1 and m_2, where $m_1 \in Z_{n_1}^*$, $m_2 \in Z_{n_2}^*$. He/She computes her/his ciphertext (C_1, C_2) by

$$C_1 \equiv m_1^2 (\mathrm{mod}\, n_1) \text{ and } C_2 \equiv m_2^2 (\mathrm{mod}\, n_2)$$

The ciphertext C_1 and C_2 in the R-RPKC can be represented as the network system as shown in Figure (3.25).

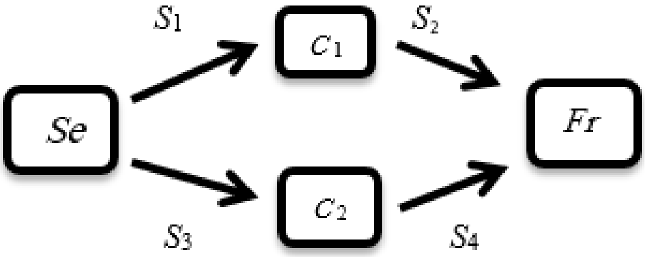


Figure 3.25. Network system of the ciphertext in the R-RPKC.

The idea with two previous cryptosystem will be applied. Two paths on the R-RPKC have been created. First one contains the C_1 of m_1 and the second one contains C_2 of m_2. The reliability of the proposed R-RPKC can be determined using PTM. The minimal path sets of proposed cryptosystem are {S_1, S_2}and {S_3, S_4}. Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.26).

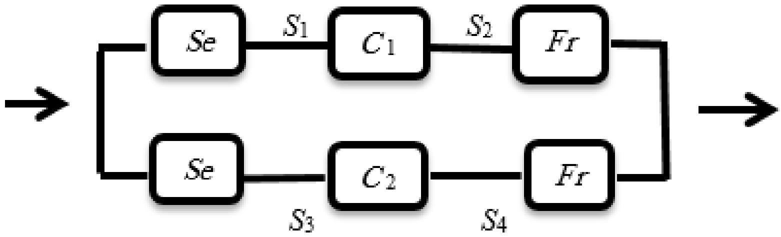


Figure 3.26. A parallel-series system of R-RPKC.

The paths for this system, in Figure (3.26), are: $P_1 = S_1S_2$ and $P_2 = S_3S_4$. The reliability Rs_j with j=1,2 of series paths computes based on the reliability R_i of subsystems S_i for i = 1, ..., 4. So, the reliability is computed as given in Equation

(3.33). The reliability of parallel system R_S is determined as given in Equation (3.34). First user wants decryption ciphertext, She/He knows the prime factors p_1, q_1 and p_2, q_2 of n_1, n_2 respectively. She/He uses the fact that determining m_1 and m_2 which is an equivalent to solve the following two congruence's for the values $m_l\,p_l$ and $m_l\,q_l$, where l =1,2

$$(m_l p_l)^2 \equiv C_h (\text{mod}\, p_l) \text{ and } (m_l q_l)^2 \equiv C_h (\text{mod} q_l).$$

She/He uses Euler's criterion to determine if C_h is a quadratic residue modulo p_l (and modulo q_l). When $p_l \equiv 3$ (mod 4), there is a simple formula to compute square roots of quadratic residues modulo p_l. Suppose C_h is a quadratic residue modulo p_l, where $p_l \equiv 3$ (mod 4), l =1,2. Then

$$\begin{aligned}\left(\pm C_h{}^{(p_l+1)/4}\right)^2 &\equiv C_h{}^{(p_l+1)/2} \left(mod\ p_l\right)\\ &\equiv C_h{}^{(p_l-1)/2} C_h \left(mod\ p_l\right)\\ &\equiv C_h \left(mod\ p_l\right).\end{aligned}$$

If C_h is a quadratic residue modulo p_l, then $C_h{}^{(p_l-1)/2} \equiv 1$ (mod p_l). Hence, the two square roots of C_h modulo p_l are $a = \pm\, C_h{}^{(p_l+1)/4}$ (mod p_l). In a similar way, the two square roots of C_h modulo q_l are $b = \pm\, C_h{}^{(q_l+1)/4}$ (mod q_l), h is number of ciphertext where m_1 and m_2 have ($+a$, $+b$), ($+a$, $-b$), ($-a$, $+b$), ($-a$, $-b$). Using the Chinese remainder theorem, the congruence's are solve.

The original plaintext of (m_1, m_2). The PSRM is used for decrypting the ciphertext and recovering the original plaintext.

The reliability that on Figure (3.27), the system has four components through two paths.

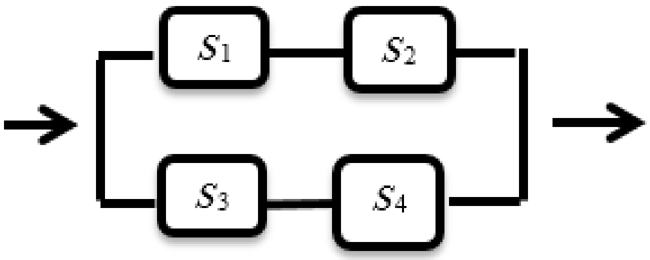


Figure 3.27. Block diagram of the plaintext in R-RPKC.

Based on the system structure given in Figure (3.27), the components S_1 and S_2, form a series subsystem which can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components $m_1 = S_1S_2$. Similarly the components S_3 and S_4, form a series subsystem that can be remodeled by a super-component referred to m_2. The super-component reliability is the product of the path components $m_2 = S_3S_4$. The block diagram of two series reductions in Figure (3.27) is transformed into Figure (3.28).

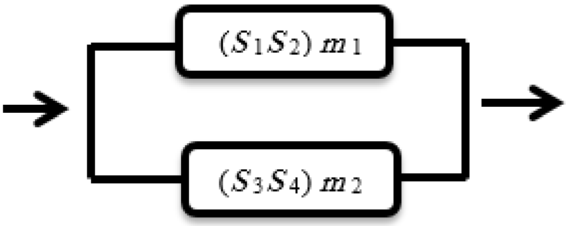


Figure 3.28. A parallel system of the plaintext in R-RPKC.

The components m_1 and m_2 in Figure (3.28) form a parallel subsystem that can be remodeled by a super-component referrs to M. The reliability of super-component M as given in Equation (3.33). The block diagram of parallel reductions in Figure (3.28) is transformed into Figure (3.29).

Figure 3.29. The original M in R-RPKC.

3.2.3.1. Study Case on the R-RPKC

First user selects the secret primes $p_1 = 67$, $q_1 = 23$, $p_2 = 59$ and $q_2 = 47$ where p_1, q_1 and p_2, $q_2 \equiv 3 \pmod 4$ with $p_1 \neq q_1$, $p_2 \neq q_2$. She/He compute her/his public modulus's $n_1 = p_1q_1 = 67\times23 = 1541$ and $n_2 = p_2q_2 = 49\times47 = 2773$. The private and public keys of the first user are ($p_1 = 67$, $q_1 = 23$), ($p_2 = 59$, $q_2 = 47$) and ($n_1 = 1541$, $n_2 = 2773$) respectively.

Second user chooses his/her plaintext M that consists of two parts $m_1 = 188$ and $m_2 = 288$, where $m_1 \in F^*_{1541}$ and $m_2 \in F^*_{2773}$. The ciphertext C_1 and C_2 computed by

$$C_1 \equiv m_1^2 (\text{mod } n_1) \equiv 188^2 (\text{mod } 1541) \equiv 1442 (\text{mod } 1541)$$

and

$$C_2 \equiv m_2^2 (\text{mod } n_2) \equiv 288^2 (\text{mod } 2773) \equiv 2527 (\text{mod } 2773).$$

The ciphertext (C_1, C_2) in the R-RPKC can be represented as the network system as shown in Figure (3.30).

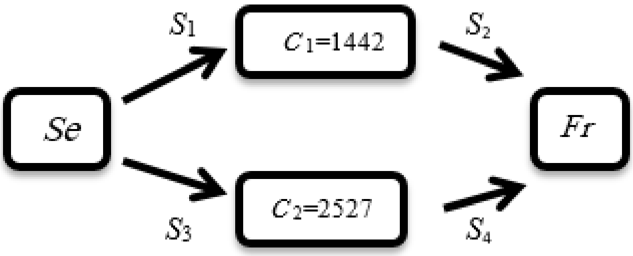


Figure 3.30. Network system of (C_1=1442, C_2=2527) in the R-RPKC.

The R-RPKC consists of two paths, the first path contains the $C_1 = 1541$ of m_1 and the second path contains $C_2 = 2527$ of m_2. The reliability of the proposed R-RPKC can be determined using PTM. The minimal path sets of proposed cryptosystem are $\{S_1, S_2\}$and $\{S_3, S_4\}$. Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.31)

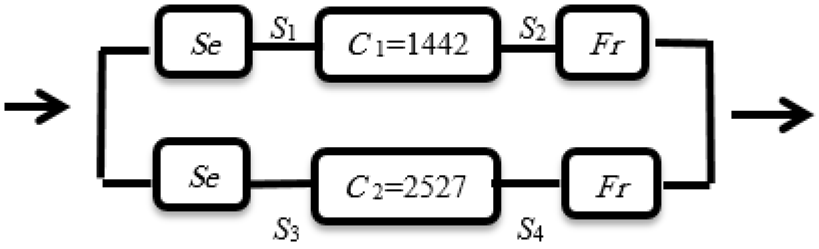


Figure 3.31. Parallel-series system of (C_1=1442, C_2=2527) in the R-RPKC.

The paths for this system, in Figure (3.31), are: P_1= S_1S_2 and P_2 = S_3S_4. The reliability Rs_j with j=1,2 of series paths computes based on the reliability R_i of subsystems S_i for i =1,2,3,4. So, the reliability is computed as given in Equation (3.33). Based on Figure (3.51), one can compute

$$Rs_1 = R_1R_2 \text{ and } Rs_2 = R_3R_4.$$

The reliability of parallel system Rs is determined as given in Equation (3.34).

$$\begin{aligned} Rs_j &= 1-[(1-Rs_1)\ (1-Rs_2)] \\ &= 1-[1-(\ R_1R_2)(1-R_3R_4)] \\ &= R_3R_4 + R_1R_2 - R_1R_2R_3R_4. \end{aligned}$$

First user wants to decryption the ciphertext, she/he knows the prime factors (p_1, q_1) and (p_2, q_2) of n_1 and n_2 respectively, so she/he can use the fact that determines m_1 and m_2 which is an equivalent to solve the following two congruence's for the values $m_l\,p_l$ and $m_l\,q_l$, where l =1,2 and h is number of ciphertext.

$$(m_l p_l)^2 \equiv C_h (\operatorname{mod} p_l) \text{ and } (m_l q_l)^2 \equiv C_h (\operatorname{mod} q_l).$$

Computing the square roots of quadratic residues modulo p_1 and modulo q_2 of m_1 are done by

$$a \equiv \pm C_1^{(p_1+1)/4} (\operatorname{mod} p_1) \equiv \pm(1442)^{67+1/4} (\operatorname{mod} 67) \equiv \pm(1442)^{17} (\operatorname{mod} 67)$$

and

$$b \equiv \pm C_1^{(q_1+1)/4} \pmod{q_1} \equiv \pm(1442)^{23+1/4} \pmod{23} \equiv \pm(1442)^6 \pmod{23}$$

then

$$a_1 \equiv +(1442)^{17} \pmod{67} \equiv 54 \pmod{67} \text{ and } a_2 \equiv -(1442)^{17} \pmod{67} \equiv 13 \pmod{67}$$

while

$$b_1 \equiv +(1442)^6 \pmod{23} \equiv 4 \pmod{23} \text{ and } b_2 \equiv -(1442)^6 \pmod{23} \equiv 19 \pmod{23}.$$

The square roots of quadratic residues modulo p_2 and modulo q_2 of m_2 are computed by

$$a' \equiv \pm C_2^{(p_2+1)/4} \pmod{p_2} \equiv \pm(2527)^{59+1/4} \pmod{59} \equiv \pm(2527)^{15} \pmod{59}$$

and

$$b' \equiv \pm C_2^{(q_2+1)/4} \pmod{q_2} \equiv \pm(2527)^{47+1/4} \pmod{47} \equiv \pm(2527)^{12} \pmod{47}$$

then

$$a'_1 \equiv +(2527)^{15} \pmod{59} \equiv 7 \pmod{59} \text{ and } a'_2 \equiv -(2527)^{12} \pmod{47} \equiv 52 \pmod{47}$$

while

$$b'_1 \equiv +(2527)^{12} \pmod{47} \equiv 6 \pmod{47} \text{ and } b'_2 \equiv -(2527)^{12} \pmod{47} \equiv 41 \pmod{47}.$$

Four roots of m_1 are determined by:

$(a_1, b_1) = (54, 4)$, $(a_1, b_2) = (54, 19)$, $(a_2, b_1) = (13, 4)$, $(a_2, b_2) = (13, 19)$.

The following congruence’s are computed by

$$\begin{aligned}
m_{a_1b_1} &\to x \equiv 54 \pmod{67}, \text{ and } x \equiv 4 \pmod{23},\\
m_{a_1b_2} &\to x \equiv 54 \pmod{67}, \text{ and } x \equiv 19 \pmod{23},\\
m_{a_2b_1} &\to x \equiv 13 \pmod{67}, \text{ and } x \equiv 4 \pmod{23},\\
m_{a_2b_2} &\to x \equiv 13 \pmod{67}, \text{ and } x \equiv 19 \pmod{23}.
\end{aligned}$$

While, m_2 has four roots which are:

$(a_1', b_1') = (7, 6), (a_1', b_2') = (7, 41), (a_2', b_1') = (52,6), (a_2', b_2') = (52,41).$

The following congruence’s are computed by

$$\begin{aligned}
&m_{a_1'b_1'} \to x \equiv 7 (\mathrm{mod}\, 59), \text{ and } x \equiv 6 (\mathrm{mod}\, 47),\\
&m_{a_1'b_2'} \to x \equiv 7 (\mathrm{mod}\, 59), \text{ and } x \equiv 41 (\mathrm{mod}\, 47),\\
&m_{a_2'b_1'} \to x \equiv 52 (\mathrm{mod}\, 59), \text{ and } x \equiv 6 (\mathrm{mod}\, 47),\\
&m_{a_2'b_2'} \to x \equiv 52 (\mathrm{mod}\, 59), \text{ and } x \equiv 41 (\mathrm{mod}\, 47).
\end{aligned}$$

Using the CRT, this congruence’s are solved by

For m_1

$$\begin{aligned}
&m_{a_1b_1}:\\
&x = 4 + 23y\\
&4 + 23y \equiv 54 (\mathrm{mod}\, 67)\\
&23y \equiv 50 (\mathrm{mod}\, 67) \qquad ,\\
&y \equiv 8 (\mathrm{mod}\, 67)\\
&\to x = 4 + 23 \times 8\\
&x = 188 \to m_1
\end{aligned}$$

$$\begin{aligned}
&m_{a_1b_2}:\\
&x = 19 + 23y\\
&19 + 23y \equiv 54 (\mathrm{mod}\, 67)\\
&23y \equiv 35 (\mathrm{mod}\, 67)\\
&y \equiv 19 (\mathrm{mod}\, 67)\\
&\to x = 19 + 23 \times 19\\
&x = 456,
\end{aligned}$$

$$
\begin{aligned}
& m_{a_2 b_1}: \\
& x = 4 + 23y \\
& 4 + 23y \equiv 13 \pmod{67} \\
& 23y \equiv 9 \pmod{67} \qquad , \\
& y \equiv 47 \pmod{67} \\
& \rightarrow x = 4 + 23 \times 47 \\
& x = 1085,
\end{aligned}
$$

$$
\begin{aligned}
& m_{a_2 b_2}: \\
& x = 19 + 23y \\
& 19 + 23y \equiv 13 \pmod{67} \\
& 23y \equiv 61 \pmod{67} \\
& y \equiv 58 \pmod{67} \\
& \rightarrow x = 19 + 23 \times 58 \\
& x = 1353.
\end{aligned}
$$

Also for m_2

$$
\begin{aligned}
& m_{a'_1 b'_1}: \\
& x = 6 + 47y \\
& 6 + 47y \equiv 13 \pmod{59} \\
& 47y \equiv 1 \pmod{59} \qquad , \\
& y \equiv 54 \pmod{59} \\
& \rightarrow x = 6 + 47 \times 55 \\
& x = 2544,
\end{aligned}
$$

$$
\begin{aligned}
& m_{a'_1 b'_2}: \\
& x = 41 + 47y \\
& 41 + 47y \equiv 7 \pmod{59} \\
& 47y \equiv 25 \pmod{59} \\
& y \equiv 52 \pmod{59} \\
& \rightarrow x = 41 + 47 \times 52 \\
& x = 2485,
\end{aligned}
$$

$$
\begin{aligned}
&m_{a'_2 b'_1}: \\
&x = 6 + 47y \\
&6 + 47y \equiv 52 (\mathrm{mod}\, 59) \\
&47y \equiv 46 (\mathrm{mod}\, 59) \quad , \\
&y \equiv 6 (\mathrm{mod}\, 59) \\
&\rightarrow x = 6 + 47 \times 6 \\
&x = 288 \rightarrow m_2,
\end{aligned}
$$

$$
\begin{aligned}
&m_{a'_2 b'_2}: \\
&x = 41 + 47y \\
&41 + 47y \equiv 52 (\mathrm{mod}\, 59) \\
&47y \equiv 11 (\mathrm{mod}\, 59) \\
&y \equiv 4 (\mathrm{mod}\, 59) \\
&\rightarrow x = 41 + 47 \times 4 \\
&x = 229.
\end{aligned}
$$

The original plaintext is m_1 = 188 and m_2 = 288. The PSRM is employed for decrypting the ciphertext and recovering the original plaintext. A system with its reliability is given in Figure (3.32) it has four components through two paths.

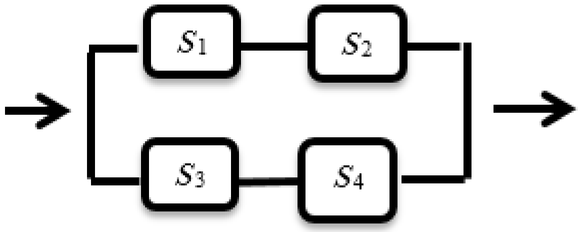


Figure 3.32. Two paths of plaintext in R-RPKC.

Based on the system structure given in Figure (3.32), the components S_1 and S_2, form a series subsystem that can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components $m_1 = R_1R_2$. Similarly the components S_3 and S_4, from a series subsystem, which can be remodeled by a super-component referred to m_2. The super-component reliability is the product of the path components $m_2 = R_3R_4$. The block diagram of two series reductions in Figure (3.32) is transformed into Figure (3.33).

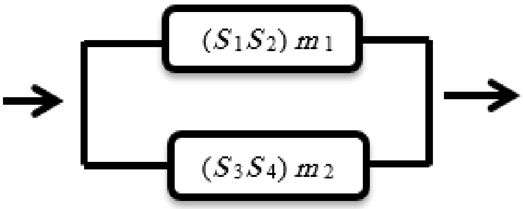


Figure 3.33. Block diagram of the plaintext after two reduction in R-RPKC.

Based on the system structure given in Figure (3.33), the components m_1 and m_2 from a parallel subsystem which can be remodeled by a super-component referred to M, the reliability of super-component M is

$$R_m = 1-(1-R_{m_1})(1-R_{m_2}) = R_{m_1} + R_{m_2} - R_{m_1}R_{m_2} = R_1R_2 + R_3R_4 - R_1R_2R_3R_4.$$

The block diagram of parallel reductions in Figure (3.33) is transformed into Figure (3.34).

Figure 3.34. The plaintext in R-RPKC.

Other computational results with various values of prime numbers *p* is presented in Table (3.3).

Table 3.4. Results of (2D-R-RPKC)

Private key(Fr)		Public key	Encryption	Decryption	
P	*Q*	N	C	Root (*a*,*b*)	*X*
991	563	557933	78911	(416,193)	204562
				(416,370)	550421
				(575,193)	$7512 \rightarrow m_1$
				(575,370)	353371
983	571	561293	49888	(931,237)	552394
				(931,334)	227021
				(52,237)	334272
				(52,334)	$8899 \rightarrow m_2$
971	547	531137	259991	(749,189)	$9488 \rightarrow m_1$
				(749,358)	427018
				(222,189)	104119
				(222,358)	521649
967	619	598573	587243	(385,197)	570915
				(385,422)	$9088 \rightarrow m_2$
				(582,197)	268224
				(582,422)	27658
947	883	567253	567769	(184,300)	189584
				(184,299)	$90149 \rightarrow m_1$
				(763,300)	477104
				(763,299)	377669
599	643	375723	153973	(431,492)	267980
				(431,151)	$94029 \rightarrow m_2$
				(452,492)	473740
				(452,151)	299789
911	907	574841	586829	(247,411)	238929
				(247,220)	486721
				(664,411)	$88120 \rightarrow m_1$
				(664,220)	335912
631	647	182172	70744	(734,53)	366255
				(734,594)	$90527 \rightarrow m_2$
				(173,53)	496302
				(173,594)	220574

3.3 The *n*-Dimension of the of Public Key Cryptosystems with PTM

This section discusses the proposed version R-EPKC, R-RSA and R-RPKC in *n*-dimensions.

3.3.1 The Reliable of EL-Gamal Public Key Cryptosystem.

This section proposes the *n*-dimension of the El-Gamal public key cryptosystem EPKC the domain parameters for *n*D-R-EPKC are: a prime *p* and a generator element *g* in a prime field F_p. A private keys (a_1, ..., a_n) is selected by first user. She/ He computes her/his public key

$$Pk_A = (PK_{A_1},...,PK_{A_n})$$

where

$$PK_1 \equiv g^{a_1} (\bmod p), \, ..., \, PK_{A_n} \equiv g^{a_n} (\bmod p).$$

Second user wants to encrypt her/his plaintext *M* and sends to first user. She/He first chooses her/his plaintext *M* and divides it into *n* parts m_1, ..., $m_n \in [2,p\text{-}1]$. An ephemeral secret keys $k_1,...,k_n \in [2,p\text{-}1]$ is chosen, The ciphertext C = $(C_1,C_2),(C_1^1,C_2^1),(C_1^2,C_2^2),...,(C_1^h,C_2^h)$ of M is computed as follows. Where *h* is number of ciphertext.

For m_1, the ciphertext (C_1, C_2) is computed by

$$C_1 \equiv g^{k_1} (\bmod p) \text{ and } C_2 \equiv m_1 (PK_{A_1})^{k_1} (\bmod p).$$

While, the ciphertext of m_2 is

$$C_1^1 \equiv g^{k_2} (\bmod p) \text{and } C_2^1 \equiv m_2 (PK_{A_2})^{k_2} (\bmod p).$$

.

.

.

and the ciphertext of m_n is

$$C_1^h \equiv g^{k_n} (\text{mod}\, p) \text{ and } C_2^h \equiv m_n (PK_{A_n})^{k_n} (\text{mod}\, p).$$

The ciphertext is $(C_1, C_2), (C_1^1, C_2^1), (C_1^2, C_2^2), ..., (C_1^h, C_2^h)$ has been sent to first user. The ciphertext in the R-EPKC can be represented as the network system as shown in Figure (3.35).

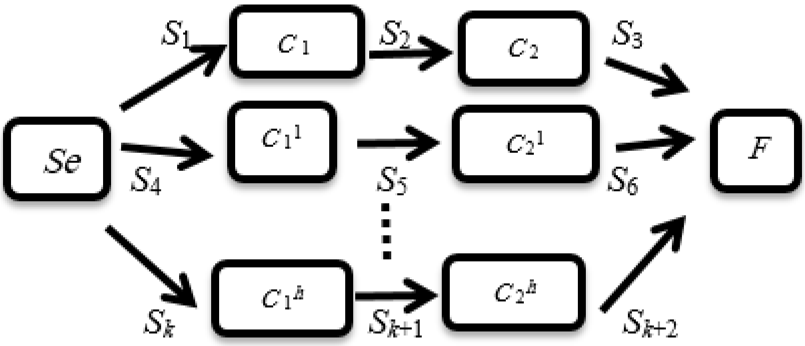


Figure 3.35. Network system of the ciphertext in *n*-dimension of R-EPKC.

The R-EPKC consists of *n* paths, the first one contains the C_1 and C_2 of m_1 and the second one consists C_1^1 and $C_2^1$of m_2 and the last one contains C_1^h and C_2^h of m_n. The reliability of the proposed R-EPKC can be determined using PTM. The minimal path sets of proposed cryptosystem are {S_1, S_2, S_3}, {S_4, S_5, S_6}, ..., {S_k, S_{k+1}, S_{k+2}} Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.36)

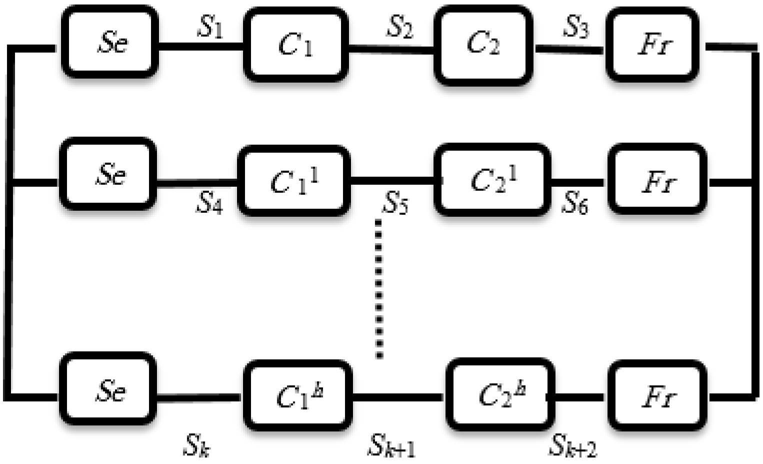


Figure 3.36. A parallel-series system of *n*-D-REPKC.

The paths for this system, in Figure (3.56), are: $P_1 = S_1S_2S_3$, $P_2 = S_4S_5S_6$, …, $P_n = S_k$-S_{k+1}-S_{k+2}. The reliability Rs_j with j=1,2, …, n of series paths computes based on the reliability R_i of subsystems S_i for i= 1, …, k. So, the reliability is computed as given in Equation (3.33). Based on Figure (3.36), the reliability of parallel system R_S is determined as given in Equation (3.34). First user receives the ciphertext (C_1, C_2), (C_1^1, C_2^1) and (C_1^h , C_2^h) so she/he wants to decrypt it and recover the plaintext m_1, …, m_n through the following calculation

$$m_1 \equiv ((C_1)^{a_1})^{-1} \times C_2 (\bmod p),\ m_2 \equiv ((C_1^1)^{a_2})^{-1} \times C_2^1 (\bmod p),\ \ldots,$$

$$m_n \equiv ((C_1^h)^{a_2})^{-1} \times C_2^h (\bmod p).$$

The original plaintext is (m_1, m_2, …, m_n). New technique to combine encrypted messages with a reliable method that is called parallel-series reduction method (PSRM) which is employed for decrypting the ciphertext and recovering the original plaintext. Suppose the system whose reliability is given in Figure (3.37).

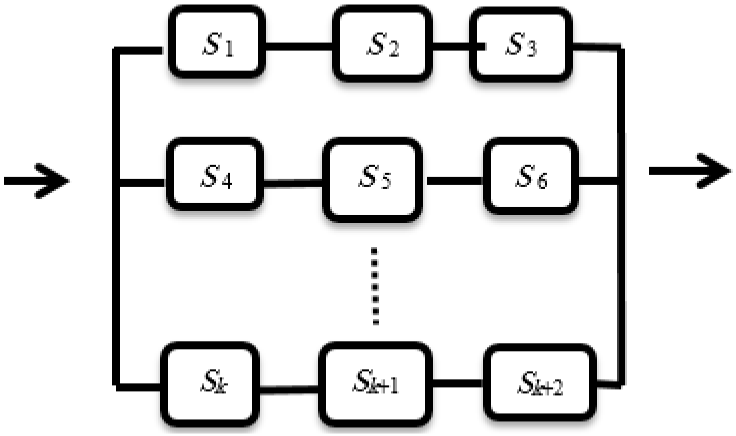


Figure 3.37. A parallel-series of the plaintext in *n*-dimension of the R-EPKC.

Based on the system structure given in Figure (3.37), the components S_1, S_2, S_3 form a series subsystem that can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components $m_1 = S_1S_2S_3$. Similarly, the components S_4, S_5, S_6 form a series subsystem which is remodeled by a super-component referred to as m_2. The super-component reliability is the product of the path components $m_2 = S_4S_5S_6$, …., and the components S_k, S_{k+1}, S_{k+2} form a series subsystem which is remodeled by a super-component referred to as m_n. The super-component reliability is the product of the path components $m_n = S_kS_{k+1}S_{k+2}$. The block diagram of a set for series reductions can be represented in given in Figure (3.37) which is transformed into Figure (3.38).

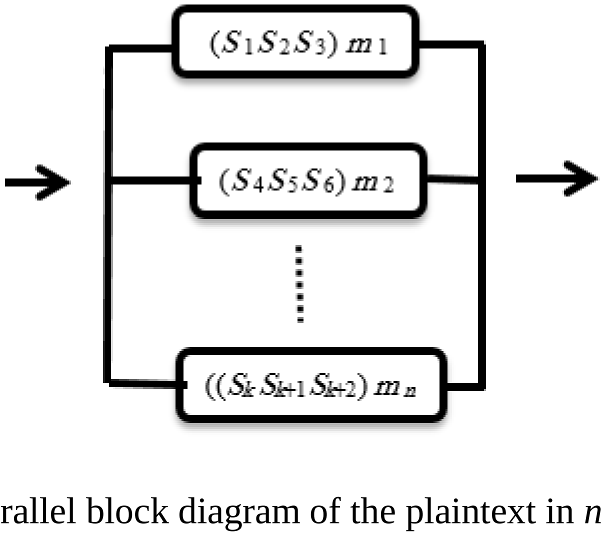


Figure 3.38. A parallel block diagram of the plaintext in *n*-dimension of R-EPKC.

Based on the system structure given in Figure (3.38), the components m_1, m_2, …, m_n form a parallel subsystem that is remodeled by a super-component referred to M. The reliability of super-component M as given in Equation (3.34). The block diagram of a set for parallel reductions in Figure (3.38) is transformed into Figure (3.39).

$(S_1 S_2 S_3 S_4 S_5 S_6 \dots S_k S_{k+1} S_{k+2})\ M$

Figure 3.39. The original plaintext in *n*-dimension of R-EPKC.

3.3.2 The Reliable of *n*-Dimension RSA Public Key Cryptosystem.

This section proposes the *n*-dimension of RSA public key cryptosystem which is called reliable RSA cryptosystem (R-RSA). The domain parameters of *n*D-R-RSA are: p_1, p_2, ..., p_n and q_1, q_2, …, q_n are large secret primes and e a public encryption exponent with the property that gcd(e, $(p_l$-1)$(q_l$-1)) = 1, which are selected by first user. She/He computes her/his public modulus $N_l = p_l\, q_l$, and compute Ø(N_l) = (p_l-1)(q_l-1), l=1,2,…,n. First user sent the public key (N_l, e) second user.

Second user wants to encrypt his/her plaintext M. He/She first chooses his/her plaintext M and divides it into n parts $m_1,..,m_n \in [1,N_l\text{-}1]$, l = 1,…, n.

He/She uses first user's public key (N_l, e) to compute the ciphertext $C = (C_1, \dots, C_h)$ of m_1, m_2, …, m_n respectively, where h number of the ciphertext by

$$C_1 \equiv m_1^e (\bmod N_1),\ C_2 \equiv m_2^e (\bmod N_2),\ \dots,\ C_h \equiv m_n^e (\bmod N_n).$$

The ciphertext is (C_1, …, C_h) has been sent to first user as the network of the ciphertext (C_1, …, C_h) and public parameters N_l as shown in Figure (3.40).

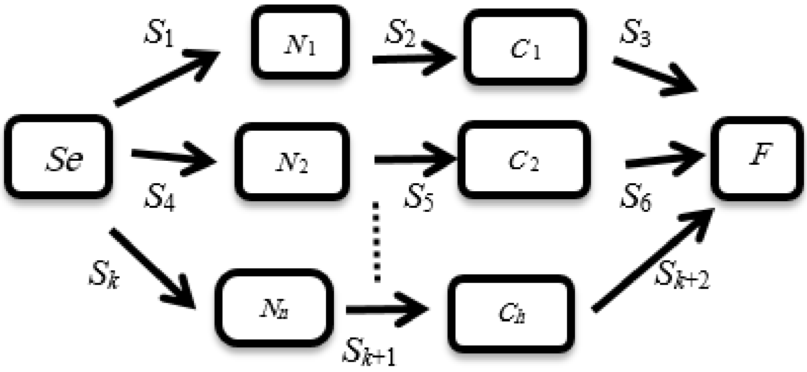


Figure 3.40. Network system of the ciphertext in *n*-dimension of the R-RSA.

First user after receiving the network cryptosystem, he/she discusses the ciphertext in Figure (3.40) as follows. The R-RSA consists of *n* paths, the first path contains the N_1 and C_1 of m_1 and the second path contains N_2 and C_2 of m_2 and the last path contains N_n and C_n of m_n. The reliability of the proposed R-RSA can be determined using PTM. The minimal path sets of proposed cryptosystem are $\{S_1, S_2, S_3\}$, $\{S_4, S_5, S_6\}$, ..., $\{S_\mathrm{k}, S_{\mathrm{k}+1}, S_{\mathrm{k}+2}\}$ Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.41)

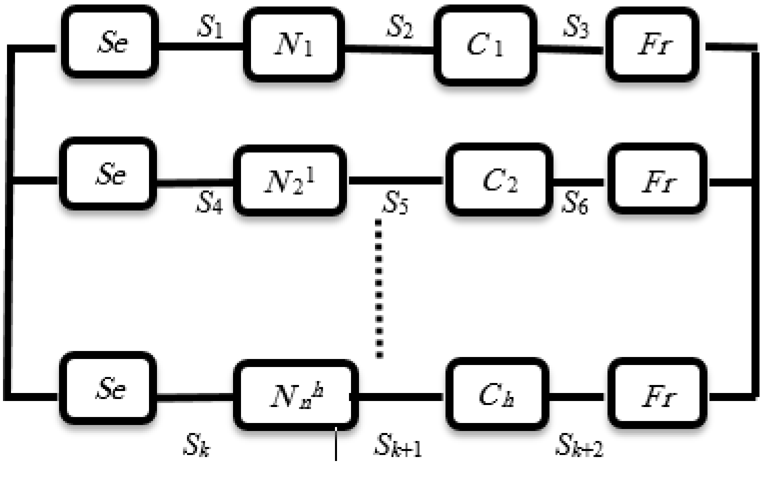


Figure 3.41. A parallel-series system of R-RSA cryptosystem in *n*-dimension.

The paths for this system, in Figure (3.41), are: $P_1 = S_1\mathrm{S}_2S_3$, $P_2 = S_4S_5S_6$, …, $P_n = S_kS_{k+1}S_{k+2}$. The reliability Rs_j with j = 1,2 of series paths computes based on the reliability R_i of subsystems S_i for i =1, …, n. So, the reliability is computed as given in Equation (2.33). The reliability of parallel system R_S is determined as given in Equation (2.34).

Upon first user receives the ciphertext, she/he wants to decrypt the ciphertext and recover the original plaintext. So, She/ He calculates the following steps, $ed_l \equiv$ 1mod(p_l-1)(q_l-1) for l=1,2, …, n can be solved, namely $d_1 \equiv e^{-1}(\bmod \varnothing(N_1))$ and $d_2 \equiv e^{-1}\bmod(\varnothing(N_2))$, …, $d_n \equiv e^{-1}\bmod(\varnothing(N_n))$ First user also calculates

$$m_1 \equiv (C_1^{d_1}(\bmod N_1) \text{ and } m_2 \equiv (C_2^{d_2}(\bmod N_2), ..., m_n \equiv (C_h^{d_n}(\bmod N_n)$$

The original plaintext is M = (m_1, m_2, …, m_n). The PSRM is used decrypting the ciphertext and recovering the original plaintext M. The system of the ciphertext in Figure (3.41) whose reliability given in Figure (3.42). The reliability system in Figure (3.42) has n path with k components.

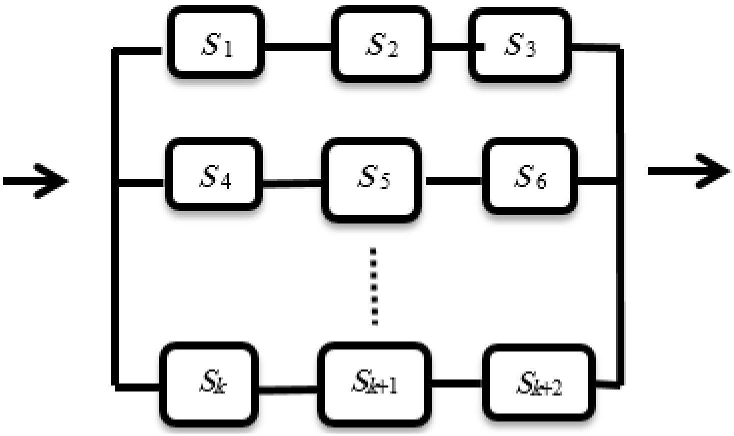


Figure 3.42. Block diagram of the plaintext in n-dimension of the R-RSA.

The components S_1, S_2, S_3 form a series subsystem that can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components m_1=$S_1S_2S_3$. Similarly, the components S_4, S_5, S_6 form a series subsystem which is remodeled by a super-component referred to as m_2. The super-component reliability is the product of the path components $m_2 = S_4S_5S_6$, …., and the components S_k, S_{k+1}, S_{k+2} form a series subsystem which is remodeled by a super-component referred to as m_n. The super-component reliability is the product of the path components m_n= $S_kS_{k+1}S_{k+2}$. The block diagram of a set for series reductions in Figure (3.42) transformed into Figure (3.43).

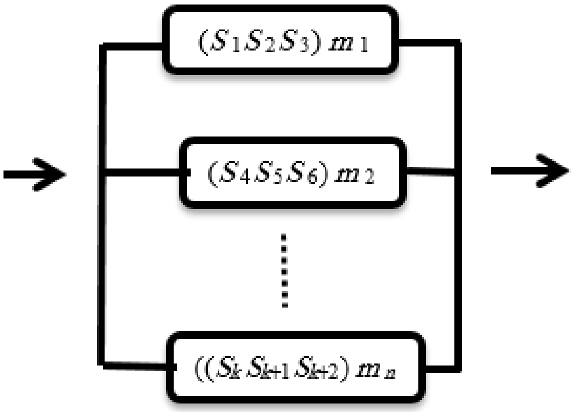


Figure 3.43. Block diagram of the plaintext after set for series reduction in R-RSA.

In Figure (3.43), the components m_1, m_2, …, m_n form a parallel subsystem that is remodeled by a super-component referred to M. The reliability of super-component M as given in Equation (2.34).

The block diagram of a set for parallel reductions in Figure (3.43) is transformed into Figure (3.44).

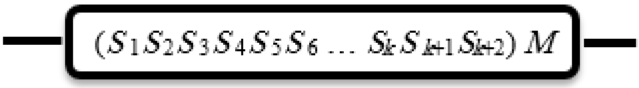


Figure 3.44. The original plaintext in *n*-dimension of the RSA.

3.3.3 Reliable *n*-Dimension Rabin Public Key Cryptosystem.

The alternative version the Rabin Cryptosystem (RPKC) has been proposed with n dimension. It is computationally secure in compare with the original one. On proposed RPKC which is also called reliable Rabin public key cryptosystem (R-RPKC), first user selects the parameters: $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_n$ as a large secret primes, where p_l and $q_l \equiv 3 \pmod 4$ with $p_l \neq q_l$. First user also computes her/his public modulus's $n_l = p_l q_l$. She/He keeps the private keys p_l and q_l

Second user knows the public keys n_l. The plaintext M is chosen and divided into n parts m_l, where $m_l \in Z^*_{n_l}$, $l = 1,2, \ldots, n$. He/She computes his/her ciphertext C_h

$$C_h \equiv m_l^2 (\bmod n_l)$$

The ciphertext C_h can be represented as the network system as shown in Figure (3.45).

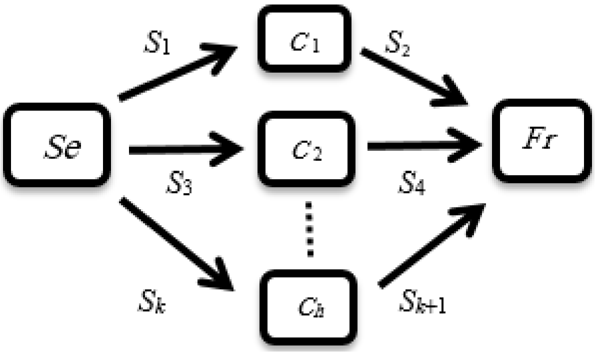


Figure 3.45. Network system of the ciphertext C_h of the R-RPKC in n-dimension.

The idea with n preivous cryptosystem will be applied. n paths on the R-RPKC have been created. First one contains the C_1 of m_1 and the second one contains C_2 of m_2 and last one contains C_h of m_n. The reliabiliy of the proposed R-RPKC can be determined using PTM. The minimal path sets of proposed cryptosystem are $\{S_1, S_2\}$, $\{S_3, S_4\}$, ..., $\{S_k, S_{k+1}\}$ Thus, the proposed cryptosystem can be represented as the parallel-series system as shown in Figure (3.46)

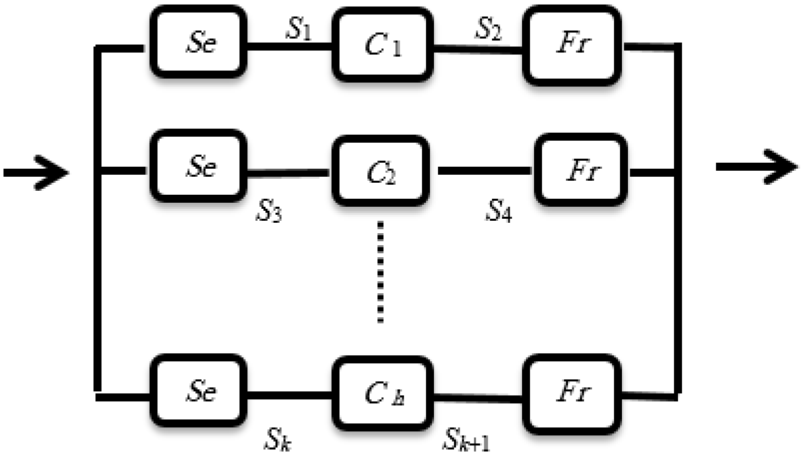


Figure 3.46. A parallel-series system of R-RPKC in n dimension.

The paths for this system, in Figure (3.46), are: $P_1 = S_1S_2$, $P_2 = S_3S_4$, …, $P_n = S_kS_{k+1}$ The reliability Rs_j with j =1,2, ..., n of series paths computes based on the reliability R_i of subsystems S_i for i =1, ..., k. So, the reliability is computed as given in Equation (2.33). The reliability of parallel system R_S is determined as given in Equation (2.34). First user wants decryption ciphertext, she/he knows the prime factors p_l, q_l of n_l, l = 1,2, …, n. She/He uses the fact that determining m_l, is equivalent to solving the following two congruence's for the values $m_l\, p_l$ and $m_l\, q_l$, where l =1,2, …, n

$$(m_l p_l)^2 \equiv C_h (\text{mod}\, p_l) \text{ and } (m_l q_l)^2 \equiv C_h (\text{mod}\, q_l).$$

She/He can use Euler's criterion to determine if C_h is a quadratic residue modulo p_l (and modulo q_l). When $p_l \equiv 3 \pmod 4$, there is a simple formula to compute square roots of quadratic residues modulo p_l. Suppose C_h is a quadratic residue modulo p_l, where $p_l \equiv 3 \pmod 4$. Then

$$\begin{aligned}\left(\pm C_h^{\,(p_l+1)/4}\right)^2 &\equiv C_h^{\,(p_l+1)/2} \,(mod\ p_l)\\ &\equiv C_h^{\,(p_l-1)/2} C_h \,(mod\ p_l)\\ &\equiv C_h \,(mod\ p_l).\end{aligned}$$

If C_h is a quadratic residue modulo p_l, then $C_h^{\,(p_l-1)/2} \equiv 1 \pmod{p_l}$. Hence, the two square roots of C_h modulo p_l are $a = \pm\, C_h^{\,(p_l+1)/4} \pmod{p_l}$. In a similar fashion, the two square roots of C_h modulo q_l are $b = \pm\, C_h^{\,(q_l+1)/4} \pmod{q_l}$, where m_l has (+a, +b), (+a, -b), (-a, +b), (-a, -b), by using the Chinese remainder theorem, the congruence's are solved.

The original plaintext of (m_1, m_2, …, m_n). The PSRM is used for decrypting the ciphertext and recovering the original plaintext.

on Figure (3.47), the system has k components through n path

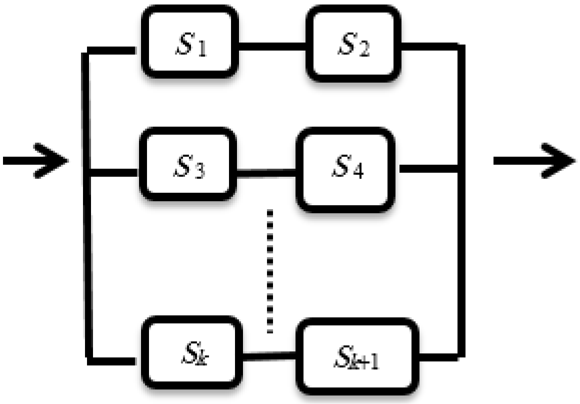


Figure 3.47. A parallel-series block diagram of the plaintext in *n*-dimension of the R-RPKC.

Based on the system structure given in Figure (3.47), the components S_1, S_2, form a series subsystem, that can be remodeled by a super-component referred to m_1. Super-component reliability is the product of the path components

$$m_1 = \prod_{i=1}^{n} R_i \text{, where } n \text{ is the number of subsystems } S_i \text{ in path } P_j.$$

Similarly the components S_3, S_4, from a series subsystem, which can be remodeled by a super-component referred to m_2. The super-component reliability is the product of the path components

$$m_2 = \prod_{i=1}^{n} R_i \text{, where } n \text{ is the number of subsystems } S_i \text{ in path } P_j.$$

, …, and the components S_k, S_{k+1}, form a series subsystem, which can be remodeled by a super-component referred to as m_n. The super-component reliability is the product of the path components

$$m_n = \prod_{i=1}^{n} R_i \text{, where } n \text{ is the number of subsystems } S_i \text{ in path } P_j.$$

the block diagram of set series reductions in Figure (3.47) is transformed into Figure (3.48).

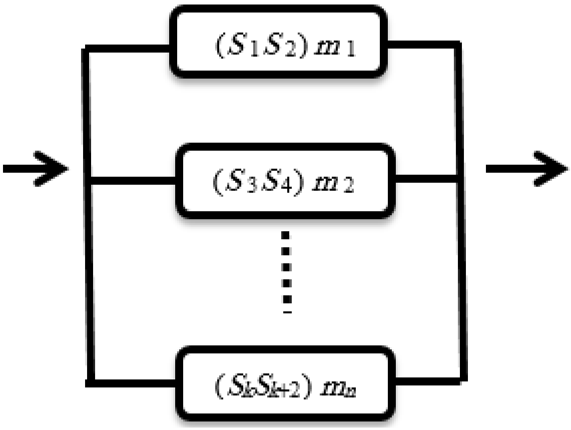


Figure 3.48. A parallel system of the plaintext after set reduction in n-dimension of the R-RPKC.

The components m_1, m_2, …, m_n in Figure (3.48) form a parallel subsystem, which can be remodeled by a super-component referred to *M*. The reliability of super-component *M* as given in Equation (2.34). The block diagram of set for parallel reductions in Figure (3.48) is transformed into Figure (3.49).

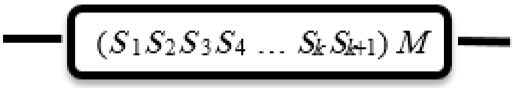


Figure 3.49. The original $M_n = (m_1, m_2, \ldots, m_n)$ in *n*-dimension of the R-RPKC.

Chapter Four

Reliability with Pivotal Decomposition Method for Some Kinds of Public Key Cryptosystems

Reliability with Pivotal Decomposition Method for Some Kinds of Public Key Cryptosystems

4.1 Introduction.

This chapter discusses modified pivotal decomposition method of new version asymmetric-key cryptosystems such as PD-EPKC, PD-RSA and PD-RPKC in 2-dimension and *n*-dimension, in more details discusses the pivotal decomposition of the proposed version of the systems are El-Gamal, Rivest–Shamir–Adleman (RSA) and Rabin. Examples are given to explain these systems, the proposed PD-EPKC, PD-RSA and PD-RPKC demonstrate an increased level of security compared to the original systems, as well as how to use the modified pivotal decomposition method in protecting ciphertexts from attackers, by deleting the failure path and creating a path for a new ciphertext. The proposed cryptosystems perfectly made and able to secure data and information.

4.2 Pivotal Decompose Public Key Cryptosystems with 2-Dimension

A new version of the Pivotal Decompose (PD) of Asymmetric -Key Cryptosystems.

4.2.1 The PD of EL-Gamal Public Key Cryptosystem.

This section proposes the 2-diminsion of the pivotal decomposition for the El-Gamal public key cryptosystem (PD-EPKC) the domain parameters for PD-EPKC are: a prime p and a generator element g in a prime field F_p, a private key $a = (a_1, a_2)$ is selected by first user. She/ He computes her/his public key

$$Pk_A = (PK_{A_1}, PK_{A_2})$$

where

$$Pk_{A_1} \equiv g^{a_1} (\bmod p) \quad \text{and} \quad PK_{A_2} \equiv g^{a_2} (\bmod p).$$

Second user wants to encrypt her/his plaintext M (study two cases a number and an english word) and sends to first user. She/He first chooses her/his plaintext M and divides it into two parts $M = (m_1, m_2)$, where $m_1, m_2 \in [2, p\text{-}1]$. An ephemeral secret key $k = (k_1, k_2)$ is chosen , where $k_1, k_2 \in [2, p\text{-}1]$. The ciphertext $C = ((C_1, C_2), (C_1', C_2'))$ of M is computed as follows.

For m_1, the ciphertext (C_1, C_2) is computed by

$$C_1 \equiv g^{k_1} (\operatorname{mod} p) \text{ and } C_2 \equiv m_1 (PK_{A_1})^{k_1} (\operatorname{mod} p).$$

While, the ciphertext of m_2 is

$$C_1' \equiv g^{k_2} (\operatorname{mod} p) \text{ and } C_2' \equiv m_2 (PK_{A_2})^{k_2} (\operatorname{mod} p).$$

The ciphertext is $C = ((C_1, C_2), (C_1', C_2'))$ has been sent to first user. The ciphertext in the PD-EPKC can be represented as the network system as shown in Figure (4.1).

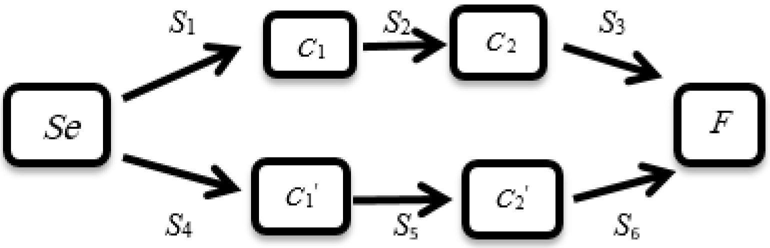


Figure 4.1. Network system of the ciphertext in the PD-EPKC.

The PD-EPKC consists of two paths, the first one contains the C_1 and C_2 of m_1 and the second one contains C_1' and C_2' of m_2. The reliability of the proposed PD-EPKC can be determined using modified pivotal decomposition method. Applying the law of total probability involves selecting a component and then calculating the reliability of the system in two partial cases, if the component fails, the change is done by deleting the path and creating a new path and calculate the reliability of the system with the success of the new component as follows.

Step1. A keystone component is chosen first. Here, the component C_i represents as the keystone component.

Step2. A component C_i can be successful or failure. If C_2 is failure, then the path is deleted. The reliability of system given by.

R(system success/component C_i failure) = P(system success/component C_i failure)

The scheme of encrypted plaintext in Figure (4.1) transformed into Figure (4.2)

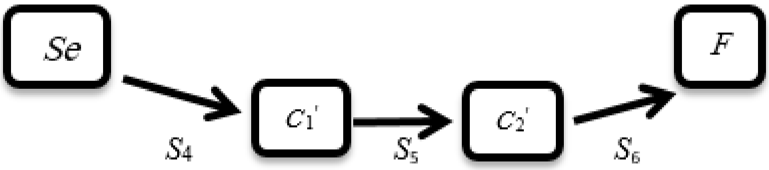


Figure 4.2. Network system of encrypted plaintext after deleted one path.

New alternative path of deleted path C_i is created to compute new C_i'' through choosing k_i' the ciphertext $C = (C_1'', C_2'')$

$$C_1'' \equiv g^{k_i^`} (\mathrm{mod}\, p) \text{ and } C_2'' \equiv m_j (Pk_{A_i})^{k_i^`} (\mathrm{mod}\, p)$$

So, a pair of the ciphertext (C_1'', C_2'') is sent to first user. The scheme of encrypted plaintext after delete and change the path in Figure (4.2) transformed into Figure (4.3).

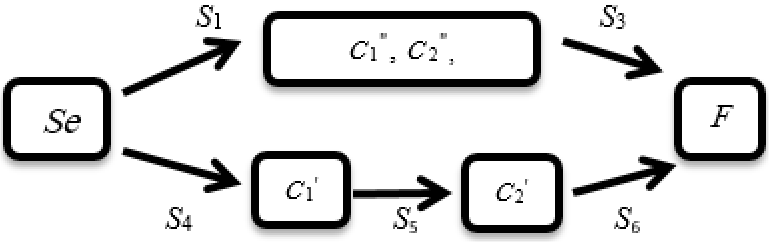


Figure 4.3. Network system of encrypted plaintext updated in PD-EPKC.

The reliability of system when component C_i'' is successful

$$R \text{ (system success/component } C_i'' \text{ is successful)}$$

$$= \text{P(system success/component } C_1'' \text{ is successful) .}$$

First user receives the ciphertext (C_1'', C_2'') and (C_1', C_2') so she/he wants to decrypt it and recover the plaintext m_1, through the following calculation

$$m_i \equiv ((C_1'')^{a_i})^{-1} \times C_2''(\bmod p).$$

and recover the plaintext m_2,

$$m_2 \equiv ((C_1')^{a_2})^{-1} \times C_2'(\bmod p).$$

The reliability of system when component C_i failure and component C_i'' successful

$$R_S = p_i\,(R\text{(system success/component } C_i'' \text{ success)} + q_i\text{(R(system success/component } C_i \text{ failure).}$$

4.2.1.1 The Computational Results on Alternative Version PD-EPKC

In this section, some examples are discussed of two cases of the modified PD-EPKC which are taken the plaintexts as numbers or as texts. These examples are considered as study cases that are discussed as follows.

4.2.1.1.1 Study Case of the Plaintext as Numbers

Let p=71 be a prime number and g = 5 be a generator element in F_{71}. First user selects her/his private key by a = (a_1, a_2) = (22, 26) such that a_1, a_2,∈ [2,70]. She/He computes her/his public key PK_A = (PK_{A_1}, PK_{A_2}) by

$$PK_{A_1} \equiv g^{a_1}(\bmod p) \equiv 5^{22}(\bmod 71) \equiv 25(\bmod 71)$$

and

$$PK_{A_2} \equiv g^{a_2}(\bmod p) \equiv 5^{26}(\bmod 71) \equiv 5(\bmod 71).$$

Second user wants to encrypt his/her plaintext M = (m_1 , m_2). He/She divided the plaintext into two parts m_1= 55 and m_2 = 15. An ephemeral secret keys is chosen by k_1= 24 and k_2 = 31 such that k_1, k_2 ∈ [2,70]. The ciphertext C = ((C_1, C_2), ($C_1^{'}$, $C_2^{'}$)) of M = (m_1, m_2) is computed for m_1 and m_2 respectively by

$$C_1 \equiv g^{k_1}(\bmod p) \equiv 5^{24}(\bmod 71) \equiv 57(\bmod 71)$$

and

$$C_2 \equiv m_1(Pk_{A_1})^{k_1}(\bmod p) \equiv 55 \times (25)^{24}(\bmod 71) \equiv 59(\bmod 71),$$

$$C_1^{'} \equiv g^{k_2}(\bmod p) \equiv 5^{31}(\bmod 71) \equiv 5(\bmod 71)$$

and

$$C_2^{'} \equiv m_2(Pk_{A_2})^{k_2}(\bmod p) \equiv 15 \times (5)^{31}(\bmod 71) \equiv 4(\bmod 71).$$

So, a pair of the ciphertext ((C_1, C_2), ($C_1^{'}$, $C_2^{'}$)) in PD-EPKC can be represented as the network system as shown in Figure (4.4) and will be sent to first user.

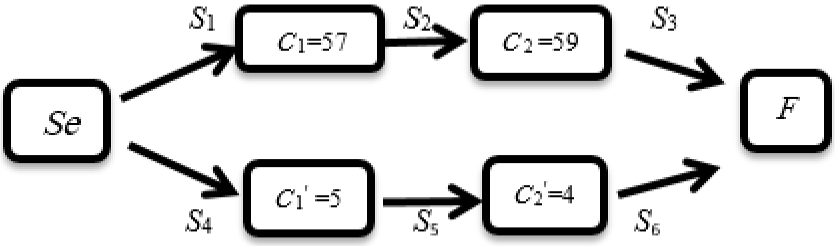


Figure 4.4. Network system of ciphertext ((C_1 = 57, C_2 = 59), ($C_1^{'}$= 5, $C_2^{'}$= 4)).

First user receives the network system diagram, she/he explains this diagram as follows. The scheme in Figure (4.4) includes two paths, the first path contains the C_1=57 and C_2 =59 of m_1 and the second path contains $C_1^{'}$= 5 and $C_2^{'}$= 4 of m_2.

The failure of one of the paths of the ciphertext is checked using the modified pivotal decomposition through the following steps:

Step1: A keystone component is chosen first. Here, component C_1 represents as the keystone component.

Step2: A component C_1 can be successful or failure. If it is failure, then the path is deleted. The reliability of system given by

$$R(\text{system success/component } C_1 \text{ failure})$$

$$= P(\text{system success/component } C_1 \text{ failure})$$

$$= R_4R_5R_6.$$

The scheme of encrypted plaintext in Figure (4.4) transformed into Figure (4.5)

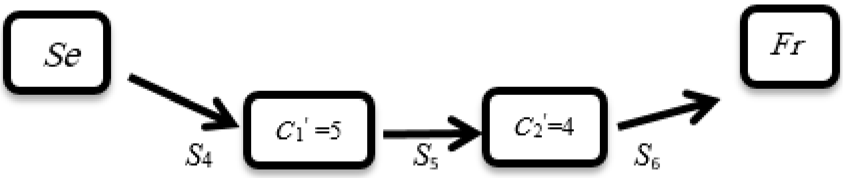


Figure 4.5. Network subsystem of ciphertext ($C_1^{'}$= 5, $C_2^{'}$= 4) after deleted the path (C_1=57, C_2 =59)

New alternative path of deleted C_i is created to compute new $C_i^{''}$ through choosing $k_1^{'}$ =37. The ciphertext $C = (C_1^{''}, C_2^{''})$

$$C_1^{''} \equiv g^{k_1^{'}} (\operatorname{mod} p) \equiv 5^{37} (\operatorname{mod} 71) \equiv 25 (\operatorname{mod} 71)$$

and

$$C_2^{''} \equiv m_1(Pk_{A_1})^{k_1^{'}}(\bmod p) \equiv 55\times(25)^{37}(\bmod 71)\equiv 11(\bmod 71).$$

So, a pair of the ciphertext ($C_1^{''}$, $C_2^{''}$) is sent to first user. The scheme of encrypted plaintext after delete and change the path in Figure (4.5) transformed into Figure (4.6).

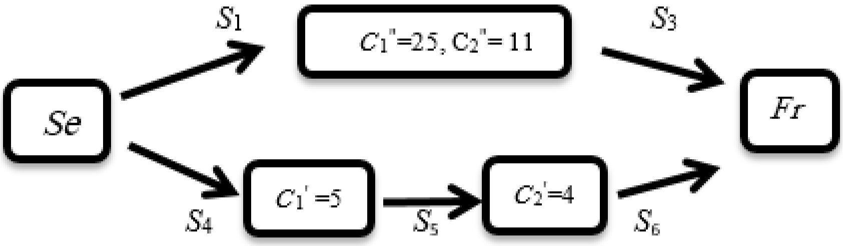


Figure 4.6. Network system of PD-EPKC after updated one path.

The reliability of system when component $C_1^{''}$ is successful

R (system success/component $C_1^{''}$ is successful)

= P(system success/component $C_1^{''}$ is successful)

$= 1-[(1-R_1R_3)(1-R_4R_5R_6)]$

$= R_1R_3+ R_4R_5R_6- R_1R_3R_4R_5R_6.$

First user receives the ciphertext (5,4), (25,11) so she/he wants to decrypt it and recover the plaintext m_1, m_2 through the following calculation

$$m_2 \equiv (C_1^{'a_2})^{-1}\times C_2^{'}(\bmod p)\equiv(5^{26})^{-1}\times 4(\bmod 71)\equiv 15(\bmod 71).$$

and

$$m_1 \equiv ((C_1^{''})^{a_1})^{-1}\times C_2^{''}(\bmod p) \equiv (25^{22})^{-1}\times 11(\bmod 71)\equiv 55(\bmod 71).$$

The reliability of system when component C_1 failure and component $C_1^{''}$ successful

$R_S = p_i$ (R(system success/component C_1"success) + q_i(R(system success/component C_1 failure)

$$= R_2[1-[(1-R_1R_3)(1-R_4R_5R_6)]]+(1-R_2)[R_4R_5R_6]$$

$$R_2[R_1R_3 + R_4R_5R_6 - R_1R_3R_4R_5R_6] + [R_4R_5R_6 - R_2R_4R_5R_6]$$

$$= R_1R_2R_3 + R_2R_4R_5R_6 - R_1R_2R_3R_4R_5R_6 + R_4R_5R_6 - R_2R_4R_5R_6$$

$$= R_1R_2R_3 + R_4R_5R_6 - R_1R_2R_3R_4R_5R_6.$$

Other computational results with various values of prime numbers p is presented in Table (4.1).

Table 4.1 Results of (2D-PD-EPKC)

Input	Private key(Fr) a_1, a_2	Public key Pk_{A1},Pk_{A2}	Private key(Se) k_1 , k_2	Encryption C_1 , C_2	Decryption m_1 , m_2
p =367	221	180	313	150 , 3	212
g =193	361	337	215	69 , 187	295
p =769	351	173	258	62 , 186	766
g =211	421	558	391	760 , 719	678
p =881	715	767	329	366 , 706	779
g =311	663	53	558	13 , 237	844
p =887	275	659	581	523 , 285	800
g =337	301	124	622	486 , 624	777
p =911	815	112	582	160 , 39	500
g =181	785	655	773	79 , 184	700

4.2.1.1.2 Study Case of the Plaintext as English Word

Let p=127 be a prime number and g = 5 be a generator element in F$_{127}$. First user selects her/his private key by a = (a_1, a_2) = (87,25) such that a_1, $a_2 \in$ [2,126] . She/He computes her/his public key PK_A = (PK_{A_1}, PK_{A_2}) by

$$PK_{A_1} \equiv g^{a_1} (\mathrm{mod}\, p) \equiv 5^{87} (\mathrm{mod} 127) \equiv 125 (\mathrm{mod} 127)$$

and

$$PK_{A_2} \equiv g^{a_2} (\mathrm{mod}\, p) \equiv 5^{25} (\mathrm{mod} 127) \equiv 10 (\mathrm{mod} 127).$$

Second user wants to encrypt his/her plaintext M which is **Gory** word such that Gory = (m_1, m_2, m_3, m_4), that is transformed into numbers by (m_1, m_2, m_3, m_4) = (71, 111, 114, 121) using the ASCII values as shown in Table (2.1). An ephemeral secret key k = (k_1, k_2) = (37,57) is chosen such that k_1, $k_2 \in$ [2,126]. The ciphertext C = ((C_1, C_2), (C_1', C_2'), (C_1', C_3'), (C_1', C_4')) of M. In more details, the ciphertexts of m_1 is computed by

$$C_1 \equiv g^{k_1} (\mathrm{mod}\, p) \equiv 5^{37} (\mathrm{mod} 127) \equiv 33 (\mathrm{mod} 127)$$

and

$$C_2 \equiv m_1 (Pk_{A_1})^{k_1} (\mathrm{mod}\, p) \equiv 71 \times (125)^{37} (\mathrm{mod} 127) \equiv 97 (\mathrm{mod} 127).$$

While, the ciphertext of m_2, m_3 and m_4 are

$$C_1' \equiv g^{k_2} (\mathrm{mod}\, p) \equiv 5^{57} (\mathrm{mod} 127) \equiv 95 (\mathrm{mod} 127),$$

$$C_2' \equiv m_2 (Pk_{A_2})^{k_2} (\mathrm{mod}\, p) \equiv 111 \times (10)^{57} (\mathrm{mod} 127) \equiv 8 (\mathrm{mod} 127),$$

$$C_3' \equiv m_3 (Pk_{A_2})^{k_2} (\mathrm{mod}\, p) \equiv 114 \times (10)^{57} (\mathrm{mod} 127) \equiv 70 (\mathrm{mod} 127)$$

and

$$C_4^{'} \equiv m_4(Pk_{A_2})^{k_2}(\bmod p) \equiv 121 \times (10)^{57}(\bmod 127) \equiv 3(\bmod 127).$$

So, pairs of the ciphertext $C = ((C_1, C_2), (C_1^{'}, C_2^{'}), (C_1', C_3'), (C_1^{'}, C_4^{'}))$ is represented by the network system as shown in Figure (4.7) and sent to first user.

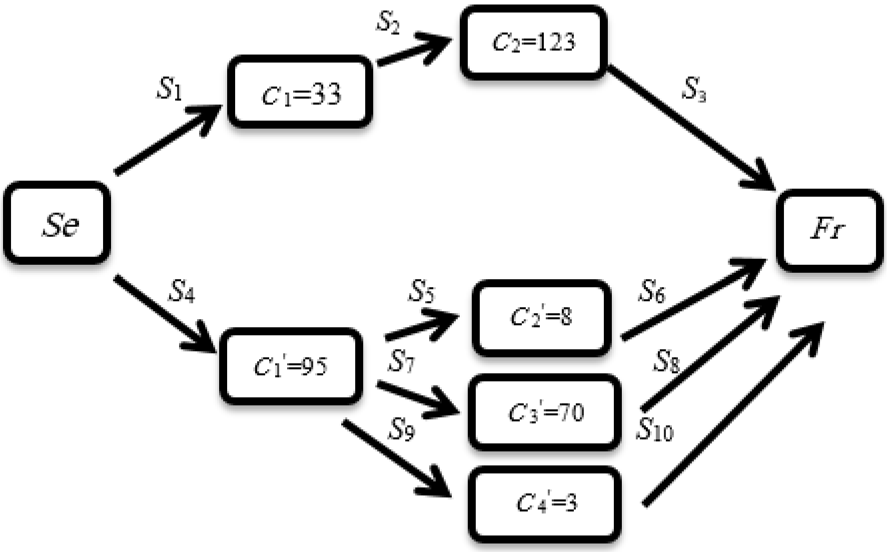


Figure 4.7. Network system of encrypted plaintext in PD-EPKC.

The PD-EPKC includes four paths, the first one contains the C_1 and C_2 of m_1 and the second one contains $C_1^{'}$ and $C_2^{'}$ of m_2, the three one contains $C_1^{'}$ and $C_3^{'}$ of m_3 and the last one contains $C_1^{'}$ and $C_4^{'}$ of m_4.

The failure of one of the paths of the ciphertext is checked using the modified pivotal decomposition through the following steps:

Step1: we first choose a keystone component. Here we choose component C_1 as the keystone component.

Step2: component C_1 can be successful or failure. If it is failure, we delete the component and the path, the reliability of subsystem given by

R(system success/component C_1 failure)= *P*(system success/component C_1 failure)

$$
\begin{aligned}
&= 1-[(1-R_4R_5R_6)(1-R_4R_7R_8)(1-R_4R_9R_{10})] \\
&= R_4R_5R_6 + R_4R_7R_8 - R_4R_5R_6R_7R_8 + R_4R_9R_{10} \\
&- R_4R_5R_6R_9R_{10} - R_4R_7R_8R_9R_{10} + R_4R_5R_6R_7R_8R_9R_{10}
\end{aligned}
$$

The scheme of encrypted plaintext in Figure (4.7) transformed into Figure (4.8)

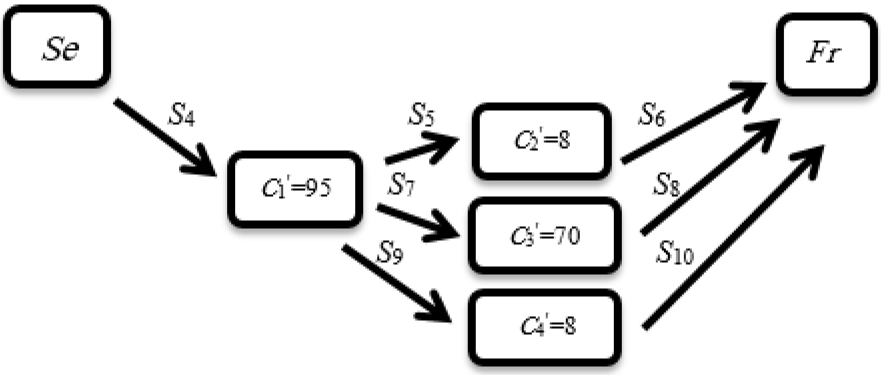


Figure 4.8. Network system of after deleted the ciphertext the (C_1=33, C_2= 123).

New alternative path of deleted path C_1 is created to compute new C_i'' through choosing k_1'=120 the ciphertext $C = (C_1'', C_2'')$

$$C_1'' \equiv g^{k_1'}(\mathrm{mod}\, p) \equiv 5^{120}(\mathrm{mod}127) \equiv 32(\mathrm{mod}127)$$

and

$$C_2'' \equiv m_1(Pk_{A_1})^{k_1'}(\mathrm{mod}\, p) \equiv 71 \times (125)^{120}(\mathrm{mod}127) \equiv 15(\mathrm{mod}127).$$

So, a pair of the ciphertext (C_1'', C_2'') is sent to first user. The scheme of encrypted plaintext after delete and change the path in Figure (4.8) transformed into Figure (4.9).

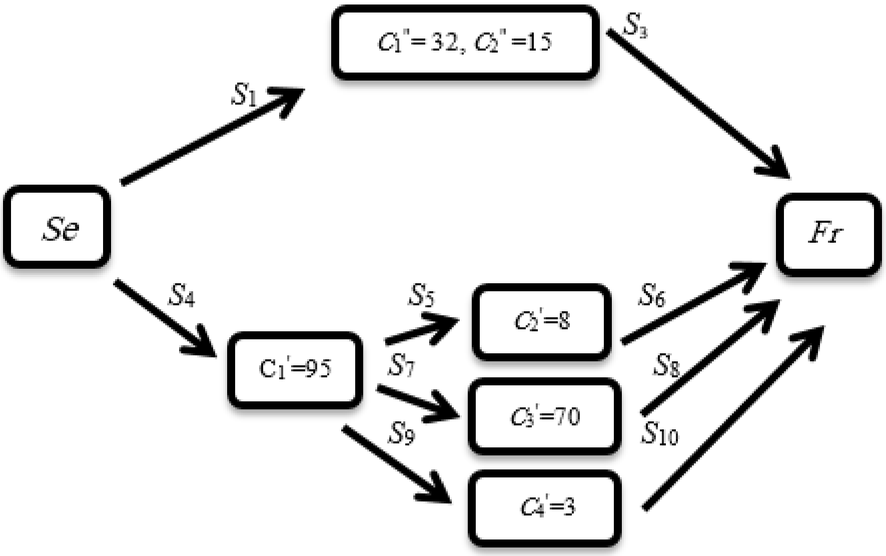


Figure 4.9. Network system of encrypted plaintext after updated encrypted plaintext ((C_1''=32, C_2''= 15).

The reliability of subsystem when component C_1'' is successful

$$R\text{ (system success/ component } C_1'' \text{ is successful)}$$

$$= P\text{(system success/ component } C_1'' \text{ is successful)}$$

$$\begin{aligned}
&=1-[(1-R_1R_3)(1-R_4R_5R_6)(1-R_4R_7R_8)(1-R_4R_9R_{10})]\\
&=R_1R_3+R_4R_5R_6-R_1R_3R_4R_5R_6+R_4R_7R_8-R_1R_3R_4R_7R_8\\
&-R_4R_5R_6R_7R_8+R_4R_9R_{10}-R_1R_3R_4R_9R_{10}-R_4R_5R_6R_9R_{10}-\\
&R_4R_7R_8R_9R_{10}+R_1R_3R_4R_5R_6R_7R_8R_9R_{10}
\end{aligned}$$

First user receives the ciphertext ((95,8), (95,70), (95,3), (32,15)), so she/he wants to decrypt it and recover the plaintext m_2, m_3, m_4, m_1 through the following calculation

$$m_2 \equiv (C_1'^{a_2})^{-1} \times C_2' (\text{mod}\, p) \equiv (95^{25})^{-1} \times 8 (\text{mod}127) \equiv 111 (\text{mod}127),$$

$$m_3 \equiv (C_1'^{a_2})^{-1} \times C_3' (\text{mod}\, p) \equiv (95^{25})^{-1} \times 70 (\text{mod}127) \equiv 114 (\text{mod}127).$$

$$m_4 \equiv (C_1'^{a_2})^{-1} \times C_4' (\text{mod}\, p) \equiv (95^{25})^{-1} \times 3 (\text{mod}127) \equiv 121 (\text{mod}127).$$

and

$$m_1 \equiv ((C_1^{"})^{a_1})^{-1} \times C_2^{"} (\bmod p) \equiv (25^{22})^{-1} \times 11 (\bmod 71) \equiv 55 (\bmod 71).$$

The reliability of system when component C_1 failure and component $C_1^{"}$ successful

$R_S = p_i$ (R(system success\component $C_1^{"}$ success) + q_i(R(system success\component C_1 failure)

$$\begin{aligned}
&= R_2[1-[(1-R_1R_3)(1-R_4R_5R_6)(1-R_4R_7R_8)(1-R_4R_9R_{10})]] \\
&+(1-R_2)[1-[(1-R_1R_3)(1-R_4R_5R_6)(1-R_4R_7R_8)(1-R_4R_9R_{10})]] \\
&= R_2[R_1R_3 + R_4R_5R_6 - R_1R_3R_4R_5R_6 + R_4R_7R_8 - R_1R_3R_4R_7R_8 \\
&-R_4R_5R_6R_7R_8 + R_4R_9R_{10} - R_1R_3R_4R_9R_{10} - R_4R_5R_6R_9R_{10} - \\
&R_4R_7R_8R_9R_{10} + R_1R_3R_4R_5R_6R_7R_8R_9R_{10}] + (1-R_2)[R_1R_3 \\
&+R_4R_5R_6 - R_1R_3R_4R_5R_6 + R_4R_7R_8 - R_1R_3R_4R_7R_8 \\
&-R_4R_5R_6R_7R_8 + R_4R_9R_{10} - R_1R_3R_4R_9R_{10} - \\
&R_4R_5R_6R_9R_{10} - R_4R_7R_8R_9R_{10} + R_1R_3R_4R_5R_6R_7R_8R_9R_{10}]
\end{aligned}$$

4.2.2 The Pivotal decompose RSA Public Key Cryptosystem.

This section proposes the 2-diminsion of the RSA public key cryptosystem which is called pivotal decompose RSA public key cryptosystem (PD-RSA). The domain parameters of PD-RSA are: p_1, p_2, q_1 and q_2 be large secret primes and e a public encryption exponent with the property that gcd(e, (p_i-1)(q_i-1)) = 1, i =1,2 which are selected by first user. She/ He computes her/his public modulus N_i, and compute Ø(N_i), namely $N_1 = p_1q_2$, $N_2 = p_2q_2$. So, Ø(N_1) = (p_1-1)(q_1-1) and Ø(N_2) = (p_2-1)(q_2-1), first user sends the public key (N_1, N_2, e) to second user.

Second user wants to encrypt his/her plaintext M. He/She first chooses his/her plaintext M and divides it into two parts M = (m_1, m_2), where $m_1 \in [1,N_1\text{-}1]$, $m_2 \in [1,N_2\text{-}1]$. He/She uses First user's public key (N_1, N_2, e) to computed the ciphertext C = (C_1, C_2) of (m_1, m_2) respectively by

$$C_1 \equiv m_1^e (\bmod N_1) \text{ and } C_2 \equiv m_2^e (\bmod N_2).$$

The ciphertext is (C_1, C_2) has been sent to first user as the network cryptosystem of the ciphertext (C_1, C_2) and public parameters N_1 and N_2 shown in Figure (4.10)

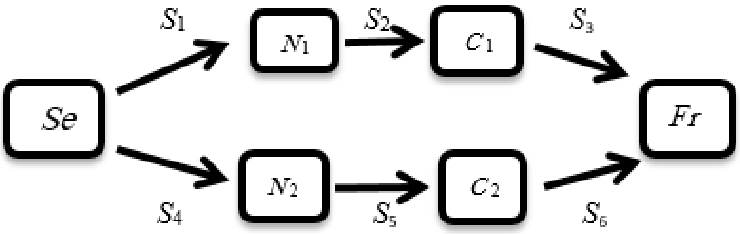


Figure 4.10. Network system of the ciphertext in the PD-RSA.

The PD-RSA consists of two paths, the first path contains the N_1 and C_1 of m_1 and the second path contains N_2 and C_2 of m_2. The reliability of the proposed PD-RSA can be determined using modified decomposition method. Applying the law of total probability involves selecting a component and then calculating the reliability of the system in two partial cases, if the component fails, the change is done by deleting the path and creating a new path and calculate the reliability of the system with the success of the new component as follows.

Step1: A keystone component is chosen first. Here, component N_2 represents as the keystone component.

Step2: A component N_2 can be successful or failure. If it is failure, then the path is deleted. The reliability of system given by

$$R(\text{system success/component } N_2 \text{ failure})$$

$$= P(\text{system success/component } N_2 \text{ failure})$$

The scheme of encrypted plaintext in Figure (4.10) transformed into Figure (4.11).

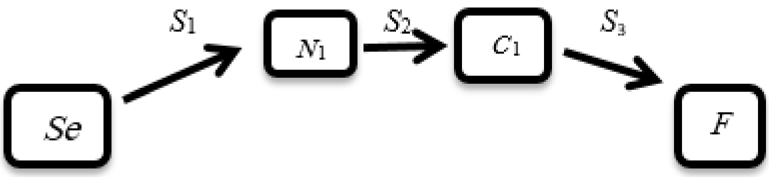


Figure 4.11. Network subsystem of encrypted plaintext in PD-RSA.

New alternative path of deleted path C$_i$ or N_i is created to compute new C$_i^{'}$ or $N_i^{'}$ through choosing $p_i^{'}$, $q_i^{'}$ where $N_i^{'}$ = p$_i^{'}$×q$_i^{'}$ and $Ø(N_i^{'}) = (p_i^{'}-1)(q_i^{'}-1)$ the ciphretext

$$C_i^{'} \equiv m_i^e (\text{mod}\, p)$$

The scheme of encrypted plaintext after delete and change the path in Figure (4.119) transformed into Figure (4.12).

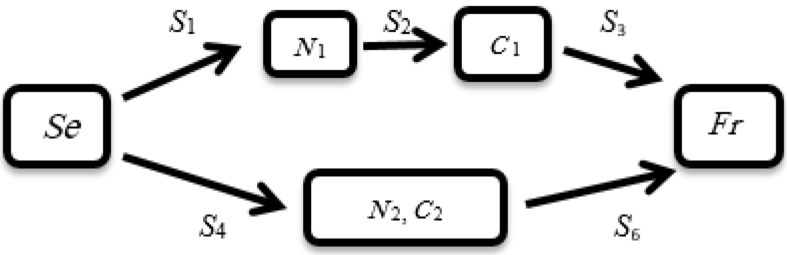


Figure 4.12. Network system of in DP-RSA after updated one path.

The reliability of system when component $C_i^{'}$ is successful

R (system success/ component $C_i^{'}$ is successful)

= P(system success/ component $C_i^{'}$ is successful).

First User knows $Ø(N_1) = (p_1-1)(q_1-1)$, $Ø(N_2^{'}) = (p_2^{'}-1)(q_2^{'}-1)$, so $ed_i \equiv 1\text{mod}$ $Ø(N_i^{'})$ for i=1,2 can be solved, namely

$$d_1 \equiv e^{-1}\text{mod}(Ø(N_1)) \text{ and } d_i^{'} \equiv e^{-1}(\text{mod}Ø(N_i^{'}))$$

Upon first user receives the ciphertext, she/ he want to decrypt the ciphertext and recover the original plaintext. So, she/ he calculates m_1 and m_i by

$$m_1 \equiv (C_1^{d_1}(\bmod N_1) \text{ and } m_i \equiv (C_i^{'})^{d_i^{'}}(\bmod N_i^{'}))$$

The reliability of system when component C_i failure and component $C_i^{''}$ successful

$R_S = p_i$ (R(system success/component $C_i^{''}$ success) + q_i(R(system success/component C_i failure).

4.2.2.1 The Study Case on the PD-RSA Cryptosystem.

First user selects her/his p_1 = 83, q_1 = 23, p_2 = 103, q_2 = 19 as the secret prime numbers. She/He selects e = 101 a public encryption exponent with the property that gcd(e, (p-1)(q-1)) = 1 She/He computes her/his public modulus N_1= p_1q_2= 83×23 =1909, N_2= p_2q_2 = 103×19 = 1957 and Ø(N) = (p -1)(q-1), Ø(N_1) = (p_1-1)(q_1-1) = 82×22 = 1804, Ø(N_2) = (p_2-1)(q_2-1) = 102×18 = 1836. The public key

(N_1, N_2, e) = (1804,1836,101).

Second user wants to encrypt his/her plaintext M. He/She divided it into two parts m_1 = 88 and m_2 = 94 , such that $m_1 \in [1, 1908]$ and $m_2 \in [1, 1956]$ Second user uses public key (N_1, N_2, e) to computed the ciphertext C_1 and C_2 of m_1 and m_2 respectively. For m_1, the ciphertext is

$$C_1 \equiv m_1^e(\bmod N_1) \equiv 88^{101}(\bmod 1909) \equiv 904(\bmod 1909).$$

While, the ciphertext of m_2 is

$$C_2 \equiv m_2^e(\bmod N_2) \equiv 94^{101}(\bmod 1957) \equiv 1728(\bmod 1957).$$

The ciphertext (C_1, C_2) and parameters N_1 and N_2 can be represented as the network system as shown in Figure (4.13).

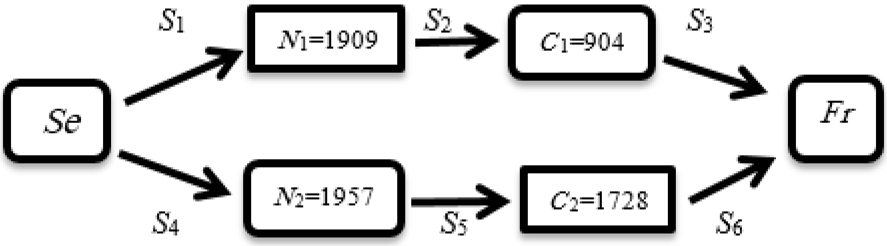


Figure 4.13. Network system of the ciphertext and public in the PD-RSA.

The PD-RSA consists of two paths, the first path contains the N_1=1909 and C_1=904 of m_1 and the second path contains N_2= 1957 and C_2 =1728 of m_2.

The failure of one of the paths of the ciphertext is checked using the modified pivotal decomposition through the following steps:

Step1: A keystone component is chosen first. Here, component N_2 represents as the keystone component.

Step2: A component N_1 can be successful or failure. If it is failure, then the path is deleted. The reliability of system given by

$$R(\text{system success/component } N_1 \text{ failure})$$

$$= P(\text{system success/component } N_1 \text{ failure})$$

$$= R_4R_5R_6.$$

The scheme of encrypted messages in Figure (4.13) transformed into Figure (4.14)

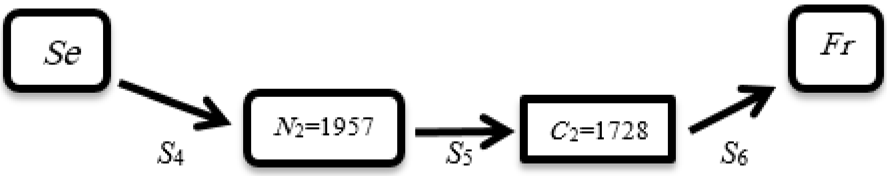


Figure 4.14. Network system of C_2 = 1728 and N_2 =2957 in PD-RSA.

New alternative path of deleted path N_1 is created to compute new $N_1^{'}$ through choosing $p_1^{'}$=41, $q_1^{'}$= 29 then $N_1^{'} = p_1^{'} \times q_1^{'}$=41×29=1189, $Ø(N_1^{'})$ = $(p_1^{'}$ -1)$(q_1^{'}$ -1) = 40×28 = 1120 and the ciphertext is

$$C_1' \equiv m_1^e (\bmod N_1') \equiv 88^{101} (\bmod 1189) \equiv 117 (\bmod 1189).$$

The scheme of encrypted plaintext after delete and change the path in Figure (4.14) transformed into Figure (4.15).

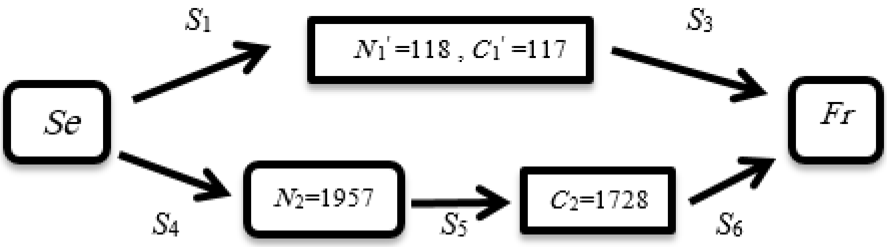


Figure 4.15. Network system of ciphertext and public updated.

The reliability of system when component N_1' is successful

R (system success/component N_1' is successful)

= P(system success/ component N_1' is successful) .

$=1-[(1-R_1R_3)(1-R_4R_5R_6)]$

$= R_1R_3+ R_4R_5R_6- R_1R_3R_4R_5R_6.$

First User knows Ø(N_1'), Ø(N_2), She/He can be solved, namely

$$d_2 \equiv e^{-1} \bmod (Ø(N_2)) \equiv 101^{-1} \bmod (1836) \equiv 509 \bmod (1836)$$

and

$$d_1' \equiv e^{-1} \bmod (Ø(N_1')) \equiv 101^{-1} \bmod (1120) \equiv 621 \bmod (1120)$$

After first user receiving the ciphertext (117,439). She/ He want to decrypt the ciphertext and recover the original plaintext. So, She/ He calculates

$$m_2 \equiv C_2^{d_2} (\bmod N_2) \equiv 1728^{509} (\bmod 1957) \equiv 94 (\bmod 1957).$$

and

$$m_1^{'} \equiv (C_1^{d_1^{'}} (\bmod N_1^{'}) \equiv 117^{621} (\bmod 1189) \equiv 88 (\bmod 1189)$$

the original plaintext of the is $M = (m_1, m_2) = (88,94)$. The reliability of system when component N_1 failure and component $N_1^{'}$ successful

$R_S = p_i$ (R(system success/component $N_1^{'}$ success) + q_i(R(system success/component N_1failure).

$$\begin{aligned}
&= R_2[1-[(1-R_1R_3)(1-R_4R_5R_6)]]+(1-R_2)[R_4R_5R_6] \\
&= R_2[R_1R_3+R_4R_5R_6-R_1R_3R_4R_5R_6]+[R_4R_5R_6-R_2R_4R_5R_6] \\
&= R_1R_2R_3+R_2R_4R_5R_6-R_1R_2R_3R_4R_5R_6+R_4R_5R_6-R_2R_4R_5R_6 \\
&= R_1R_2R_3+R_4R_5R_6-R_1R_2R_3R_4R_5R_6.
\end{aligned}$$

Other computational results with various values of prime numbers p is presented in Table (4.2).

Table 4.2 Results of (2D-PD-RSA)

Private key(Fr)		Public key		Ø(N)	Encryption C	Decryption	
P	*Q*	*N*	*e*			*d*	*m*
751	571	428821	383	427500	306874	279047	1250
421	607	255547		254520	248640	77087	2400
641	479	307039	277	305920	43859	254013	2888
757	433	327781		326592	209993	145021	5994
977	863	843151	409	841312	680620	2057	8888
809	733	592997		591456	69081	267529	8080
761	151	114911	257	114000	50341	83393	2100
419	389	162991		162184	36829	85825	3445
619	863	534197	353	532716	491116	273149	2023
457	727	332239		331056	30567	131297	2022

4.2.3 Pivotal Decompose Rabin Public Key Cryptosystem.

The alternative version of the Rabin public key Cryptosystem, (RPKC) it is computationally secure in compare with the original one. On proposed RPKC which is also called pivotal decompose Rabin public key cryptosystem (PD-RPKC), first user selects the parameters: p_1, p_2, q_1 and q_2, as a large secret primes, where p_1, q_1 and p_2, $q_2 \equiv 3 \pmod 4$ with $p_1 \neq q_1$, $p_2 \neq q_2$. First user also computes her/his public modulus's n_1 and n_2 where, $n_1 = p_1q_1$, $n_2 = p_2q_2$. She/He keeps the private key p_1, p_2, q_1 and q_2.

Second user knows the public keys n_1 and n_2. The plaintext M of his/her is chosen and divided into two parts m_1 and m_2, where $m_1 \in Z^*_{n_1}$ and $m_2 \in Z^*_{n_2}$. He/She computes his/her ciphertext (C_1, C_2) by

$$C_1 \equiv m_1^2 (\mathrm{mod}\, n_1) \text{ and } C_2 \equiv m_2^2 (\mathrm{mod}\, n_2)$$

The ciphertext (C_1, C_2) in the PD-RPKC can be represented as the network system as shown in Figure (4.16).

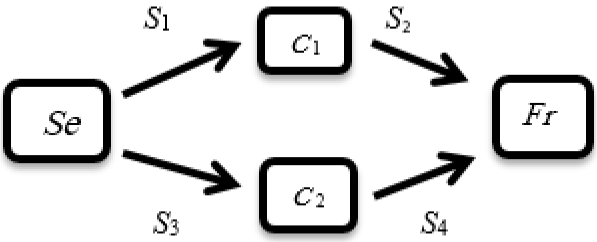


Figure 4.16. Network system of the ciphertext C_1 and C_2 in the PD-RPKC.

The idea with two preivous cryptosystem will be applied. Two paths on the PD-RPKC have been created first path contains the C_1 of m_1 and the second path contains C_2 of m_2. The reliability of the proposed PD-RPKC can be determined using modified pivotal decomposition method. Applying the law of total probability involves selecting a component and then calculating the reliability of the system in two partial cases, if the component fails, the change is done by deleting the path and creating a new path and Calculate the reliability of the system with the success of the new component as follows.

Step1: A keystone component is choses first. Here, the component C_i represents as the keystone component.

Step2: A component C_i can be successful or failure. If C_i is failure, then the path is deleted. The reliability of system given by

$$R(\text{system success/component } C_i \text{ failure})$$

$$= P(\text{system success/component } C_i \text{ failure})$$

The scheme of encrypted messages in Figure (4.16) transformed into Figure (4.17)

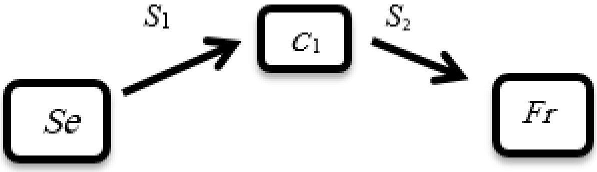


Figure 4.17. Network system of ciphertext C_1 in DP-RPKC.

New alternative path of deleted path C_i is created to compute new $C_i^{'}$ through choosing $p_i^{'}$ and $q_i^{'}$ where p_i, $q_i \equiv 3 \pmod 4$ and $p_i \neq q_i$, $n_i = p_i q_i$ with $n_i = p_i q_i$.

The ciphertext $C_i^{'}$ is computed by

$$C_i^{'} \equiv m_i \,(\text{mod}\, n_i^{'}).$$

The scheme of encrypted messages after delete and change the path in Figure (4.17) transformed into Figure (4.18).

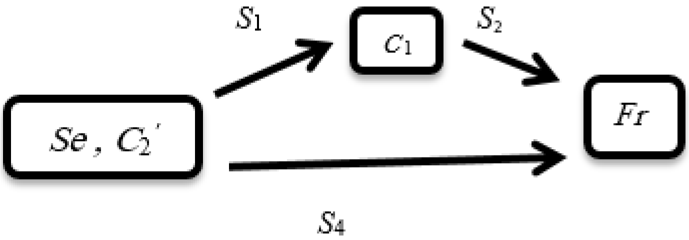


Figure 4.18. Network system of ciphertexts C$_1$ and updated $C_2^{'}$.

The reliability of system when component $C_i^{'}$ is successful

$$R \text{ (system success/component } C_i^{'} \text{ is successful)}$$

$$= \text{P(system success/ component } C_1^{'} \text{ is successful).}$$

First user wants decryption ciphertext, She/He knows the prime factors p_1, q_1 and p_2, q_2 of n_1 and n_2 respectively, she/he solves the following two congruence's

$$(m_l p_l)^2 \equiv C_h (\bmod p_l) \text{ and } (m_l q_l)^2 \equiv C_h (\bmod q_l).$$

She/He uses the Euler's criterion to determine if C_h is a quadratic residue modulo p_l (and modulo q_l) or not When $p_l \equiv 3 \pmod 4$, there is a simple formula to compute square roots of quadratic residues modulo p_l. Suppose C_h is a quadratic residue modulo p_l, where $p_l \equiv 3 \pmod 4$, l = 1,2 and h is number of ciphertext. Then

$$\begin{aligned}\left(\pm C_h^{\;(p+1)/4}\right)^2 &\equiv C_h^{\;(p_l+1)/2} \left(mod\ p_l\right)\\ &\equiv C_h^{\;(p_l-1)/2} C_h \left(mod\ p_l\right)\\ &\equiv C_h \left(mod\ p_l\right).\end{aligned}$$

If C_h is a quadratic residue modulo p_l, then $C_h^{\;(p_l-1)/2} \equiv 1 \pmod{p_l}$. Hence, two square roots of C_h modulo p_l are $a = \pm\, C_h^{\;(p_l+1)/4} \bmod p_l$. In a similar way, two square roots of C_h modulo q_l are $b =\pm\, C_h^{\;(q_l+1)/4} \bmod q_l$, with m_1 and m_2 has $(+a, +b)$, $(+a, -b)$, $(-a, +b)$, $(-a, -b)$, l = 1,2 and h is number of ciphertext. This congruence's are solved using the Chinese remainder theorem (CRT). The reliability of system when component C_i failure and component $C_i^{'}$ successful

$R_S = p_i\,(R(\text{system success/component } C_i^{'} \text{ success}) + q_i(R(\text{system success/component } C_i \text{ failure}).$

4.2.3.1 Study Case on the PD-RPKC.

Let $p_1 = 167$, $q_1 = 151$, $p_2 = 163$ and $q_2 = 107$, be a secret prime numbers are selected by first user, where p_1, q_1 and p_2, $q_2 \equiv 3 \pmod 4$ and $p_1 \neq q_1$, $p_2 \neq q_2$. She/He compute her/his public modulus's n_1 and n_2 respectively, with, $n_1 = p_1q_1 = 167\times151 = 25217$ and $n_2 = p_2q_2 = 163\times107 = 17441$. First user sends the public keys $n_1 = 25217$ and $n_2 = 17441$ to Second user. Second user know the public keys n_1 and n_2. She/He chooses the plaintext M that consist of two parts $m_1 = 5113$ $m_2 = 4421$, where $m_1 \in Z_{n_1}^*$ and $m_2 \in Z_{n_2}^*$ She/He computes her/his ciphertext $C = (C_1, C_2)$ by squaring her/his plaintext $M = (5113,4421)$ modulo $(25217,17441)$ respectively, the ciphertext (C_1, C_2)

$$C_1 \equiv m_1^2 (\bmod\, n_1) \equiv (51113)^2 (\bmod\, 25217) \equiv 17957 (\bmod\, 25217)$$

and

$$C_2 \equiv m_2^2 (\bmod\, n_2) \equiv (4421)^2 (\bmod 17441) \equiv 11321 (\bmod 17441).$$

The ciphertext (C_1, C_2) in the PD-RPKC can be represented as the network system as shown in Figure (4.19).

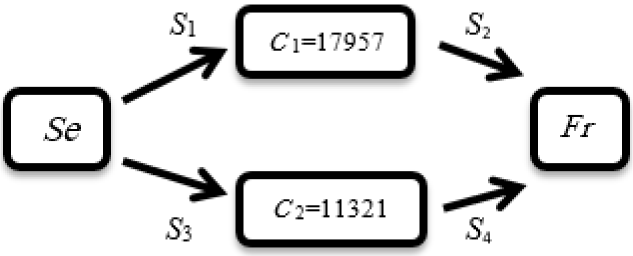


Figure 4.19. Network system of the ciphertext ($C_1 = 17957$, $C_2 = 11321$) in the PD-RPKC.

The PD-RPKC consists of two paths, the first path contains the $C_1 = 17957$ of m_1 and the second path contains $C_2 = 11321$ of m_2. The failure of one of the paths of the ciphertext is checked using the modified pivotal decomposition through the following steps:

Step1: A keystone component has been chosen by C_2.

Step2: A component C_2 can be successful or failure. If it is failure, the path of $C_2$is deleted. The reliability of system is determined by

$$R(\text{system success/component } C_2 \text{ failure})$$

$$= P(\text{system success/component } C_2 \text{ failure})$$

$$= R_1 R_2$$

The scheme of encrypted messages in Figure (4.19) transformed into Figure (4.20)

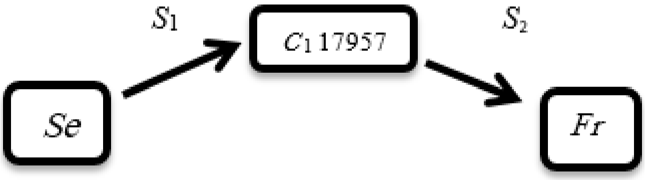


Figure 4.20. Network subsystem of ciphertext C_1= 17957 in the PD-RPKC.

New alternative path is created instead of the deleted path C_2, so the sub-ciphertext is computed with the parameters p_2' =227 and q_2' = 179 where p_2' and $q_2' \equiv 3$ (mod 4) with $p_2' \neq q_2'$ and $n_2'= p_2'q_2'$= 227×179 = 40633. Thus,

$$C_2' \equiv m_2^2 (\text{mod}\, n_2') \equiv (4421)^2 (\text{mod}\, 40633) \equiv 768 (\text{mod}\, 40633).$$

The scheme of encrypted messages after delete and change the path in Figure (4.20) transformed into Figure (4.21).

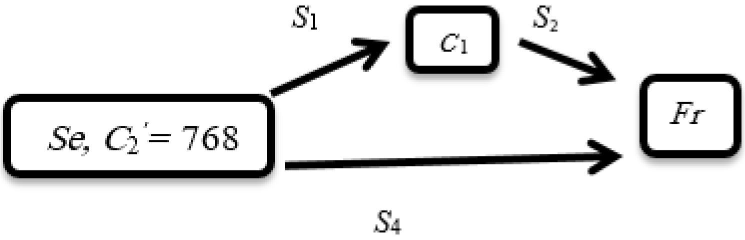


Figure 4.21. Network system of ciphertexts C_1= 17957 and updated C_2'=768.

The reliability of subsystem when component C_2' is successful

R (system success/component C_2' is successful)

= P(system success/component C_2' is successful)

$$=1-[(1-R_1R_2)(1-R_4)]$$
$$=R_1R_2+R_4-R_1R_2R_4.$$

First user wants decryption the ciphertext so, she/he knows the prime factors p_1, q_1 and p_2, q_2 of n_1 and n_2 respectively. Hence, she/he solves two congruence's for the values $m_l\, p_l$ and $m_l\, q_l$, where l =1,2 and h is number of ciphertext.

$$(m_l p_l)^2 \equiv C_h (\bmod p_l) \text{ and } (m_l q_l)^2 \equiv C_h (\bmod q_l).$$

Computing the square roots of quadratic residues modulo p_1 and modulo q_1 of m_1

$$a \equiv \pm C_1^{(p_1+1)/4} (\bmod p_1) \equiv \pm(5113)^{167+1/4} (\bmod 167) \equiv \pm(5113)^{42} (\bmod 167)$$

and

$$b \equiv \pm C_1^{(q_1+1)/4} (\bmod q_1) \equiv \pm(5113)^{151+1/4} (\bmod 151) \equiv \pm(5113)^{38} (\bmod 151)$$

then

$$a_1 \equiv +(5113)^{42} (\bmod 167) \equiv 64 (\bmod 167) \text{ and } a_2 \equiv -(5113)^{42} (\bmod 167) \equiv 103 (\bmod 167)$$

While,

$b_1 \equiv +(5113)^{38}(\mathrm{mod}151) \equiv 21(\mathrm{mod}151)$ and $b_2 \equiv -(5113)^{38}(\mathrm{mod}151) \equiv 130(\mathrm{mod}151)$.

The square roots of quadratic residues modulo p_2 and modulo q_2 of m_2

$$a'' \equiv \pm(C_2')^{(p_2'+1)/4}(\mathrm{mod}\, p_2') \equiv \pm(768)^{227+1/4}(\mathrm{mod}\,227) \equiv \pm(768)^{57}(\mathrm{mod}\,227)$$

and

$$b'' \equiv \pm(C_2')^{(q_2'+1)/4}(\mathrm{mod} q_2') \equiv \pm(768)^{179+1/4}(\mathrm{mod}179) \equiv \pm(768)^{45}(\mathrm{mod}179)$$

then

$a_1'' \equiv +(768)^{57}(\mathrm{mod}\,227) \equiv 108(\mathrm{mod}\,227)$ and $a_2'' \equiv -(768)^{57}(\mathrm{mod}\,227) \equiv 119(\mathrm{mod}\,227)$

While,

$b_1'' \equiv +(768)^{45}(\mathrm{mod}179) \equiv 125(\mathrm{mod}179)$ and $b_2'' \equiv -(768)^{45}(\mathrm{mod}179) \equiv 54(\mathrm{mod}179)$.

Four roots of m_1 are determined by

(a_1, b_1) = (64, 21), (a_1, b_2) = (64, 130), (a_2, b_1) = (103, 21), (a_2, b_2) = (103, 130).
The following congruence's are computed

$$\begin{aligned}
m_{a_1b_1} &\rightarrow x \equiv 64(\mathrm{mod}167), \text{ and } x \equiv 21(\mathrm{mod}151),\\
m_{a_1b_2} &\rightarrow x \equiv 64(\mathrm{mod}167), \text{ and } x \equiv 130(\mathrm{mod}151),\\
m_{a_2b_1} &\rightarrow x \equiv 103(\mathrm{mod}167), \text{ and } x \equiv 21(\mathrm{mod}151),\\
m_{a_2b_2} &\rightarrow x \equiv 103(\mathrm{mod}167), \text{ and } x \equiv 130(\mathrm{mod}151).
\end{aligned}$$

While, m_2 has four roots which are

(e_1, f_1) = (108, 125), (e_1, f_2) = (108, 54), (e_2, f_1) = (119,125), (e_2, f_2) = (119,54).

The following congruence's are computed

$$m_{e_1f_1} \rightarrow x \equiv 108(\bmod 227), \text{ and } x \equiv 125(\bmod 179)$$
$$m_{e_1f_2} \rightarrow x \equiv 108(\bmod 227), \text{ and } x \equiv 54(\bmod 179)$$
$$m_{e_2f_1} \rightarrow x \equiv 119(\bmod 227), \text{ and } x \equiv 125(\bmod 179)$$
$$m_{e_2f_2} \rightarrow x \equiv 119(\bmod 227), \text{ and } x \equiv 54(\bmod 179).$$

Using the CRT, this congruence's are solved by:

For m_1

$$\begin{aligned}
&m_{a_1b_1}: \\
&x = 21+151y \\
&21+151y \equiv 64(\bmod 167) \\
&151y \equiv 43(\bmod 167) \qquad , \\
&y \equiv 133(\bmod 167) \\
&\rightarrow x = 21+151\times 133 \\
&x = 20104
\end{aligned}$$

$$\begin{aligned}
&m_{a_1b_2}: \\
&x = 130+151y \\
&130+151y \equiv 64(\bmod 167) \\
&151y \equiv 101(\bmod 167) \\
&y \equiv 25(\bmod 167) \\
&\rightarrow x = 130+151\times 25 \\
&x = 3905,
\end{aligned}$$

$$\begin{aligned}
&m_{a_2b_1}: \\
&x = 21+151y \\
&21+151y \equiv 103(\bmod 167) \\
&151y \equiv 82(\bmod 167) \qquad , \\
&y \equiv 141(\bmod 167) \\
&\rightarrow x = 21+151\times 141 \\
&x = 21312,
\end{aligned}$$

$$\begin{aligned}&m_{a_2b_2}:\\&x=130+151y\\&130+151y\equiv 103(\mathrm{mod}\,167)\\&151y\equiv 140(\mathrm{mod}\,167)\\&y\equiv 33(\mathrm{mod}\,167)\\&\rightarrow x=130+151\times 33\\&x=5113\rightarrow m_1.\end{aligned}$$

Also for m_2

$$\begin{aligned}&m_{e_1f_1}:\\&x=125+179y\\&125+179y\equiv 108(\mathrm{mod}\,227)\\&179y\equiv 210(\mathrm{mod}\,227)\qquad\qquad ,\\&y\equiv 24(\mathrm{mod}\,227)\\&\rightarrow x=125+179\times 24\\&x=4421\rightarrow m_2,\end{aligned}$$

$$\begin{aligned}&m_{e_1f_2}:\\&x=54+179y\\&54+179y\equiv 108(\mathrm{mod}\,227)\\&179y\equiv 54(\mathrm{mod}\,227)\\&y\equiv 161(\mathrm{mod}\,227)\\&\rightarrow x=54+179\times 161\\&x=28873,\end{aligned}$$

$$\begin{aligned}&m_{e_2f_1}:\\&x=125+179y\\&125+179y\equiv 119(\mathrm{mod}\,227)\\&179y\equiv 221(\mathrm{mod}\,227)\qquad\qquad ,\\&y\equiv 142(\mathrm{mod}\,227)\\&\rightarrow x=125+179\times 142\\&x=25543,\end{aligned}$$

$$\begin{aligned}
&m_{e_2 f_2}:\\
&x = 54 + 179y\\
&54 + 179y \equiv 119 (\bmod 227)\\
&179y \equiv 65 (\bmod 227)\\
&y \equiv 202 (\bmod 227)\\
&\rightarrow x = 54 + 179 \times 202\\
&x = 36212.
\end{aligned}$$

The reliability of system when component C_2 failure and component $C_2{}'$ successful

$R_S = p_i$ (R(system success/component $C_1{}'$ success) + q_i(R(system success/component C_1 failure)

$$\begin{aligned}
&= R_3[1-[(1-R_1R_2)(1-R_4)]] + (1-R_3)[R_1R_2]\\
&= R_3[R_1R_2 + R_4 - R_1R_2R_4] + (1-R_3)[R_1R_2]\\
&= R_1R_2R_3 + R_3R_4 - R_1R_2R_3R_4 + R_1R_2 - R_1R_2R_3\\
&= R_1R_2 + R_3R_4 - R_1R_2R_3R_4.
\end{aligned}$$

Other computational results with various values of prime numbers p is presented in Table (4.3).

Table 4.3 Results of (2D-PD-RPKC)

Private key(Fr)		Public key	Encryption	Decryption	
P	q	n	C	Root (a,b)	X
863	523	451349	297322	(313,287)	161894
				(313,236)	$25340 \to m_1$
				(550,287)	426009
				(550,236)	448498
811	491	398201	352242	(100,237)	365050
				(100,254)	381270
				(711,237)	$16931 \to m_2$
				(711,254)	33151
859	503	432077	76152	(175,88)	379853
				(175,415)	219220
				(684,88)	212857
				(684,415)	$52224 \to m_1$
751	463	347713	247937	(180,130)	2487611
				(180,333)	$11445 \to m_2$
				(571,130)	336268
				(571,333)	98952
839	499	418661	239277	(578,16)	316881
				(578,483)	351280
				(261,16)	$67381 \to m_1$
				(261,483)	101780
751	487	365737	257510	(500,53)	274234
				(500,434)	274615
				(251,53)	$91122 \to m_2$
				(251,434)	221045
827	367	303509	242768	(710,149)	54465
				(710,218)	221519
				(117,149)	$81990 \to m_1$
				(117,218)	249044
683	479	327157	129278	(337,300)	56343
				(337,179)	266024
				(346,300)	$61133 \to m_2$
				(346,179)	270814

4.3 The *n*-Dimension of the Public Key Cryptosystems with Pivotal Decomposition.

In this section, the proofs of the proposed of PD-EPKC, PD-RSA and PD-RPKC in *n* dimensions are discussed as follows.

4.3.1 The PD of EL-Gamal Public Key Cryptosystem.

This section proposes the *n*-dimension of the El-Gamal public key cryptosystem (EPKC) the domain parameters for *n*D-PDEPKC are: a prime *p* and a generator element *g* in a prime field F_p. A private keys (a_1, ..., a_n) is selected by first user. She/ He computes her/his public key

$$Pk_A = (PK_{A_1},...,PK_{A_n})$$

where

$$PK_1 \equiv g^{a_1} (\bmod p),..., \ PK_{A_n} \equiv g^{a_n} (\bmod p).$$

Second user wants to encrypt her/his plaintext *M* and sends to first user. She/He first chooses her/his plaintext *M* and divides it into n parts $m_1,..,m_n \in[2,p-1]$. An ephemeral secret keys $k_1,...,k_n \in[2, p-1]$ is chosen, The ciphertext *C* = $(C_1,C_2),(C_1^1,C_2^1),(C_1^2,C_2^2),...,(C_1^h,C_2^h)$ of *M* is computed as follows. Where *h* is number of ciphertext.

For m_1, the ciphertext (C_1, C_2) is computed by

$$C_1 \equiv g^{k_1} (\bmod p) \text{ and } C_2 \equiv m_1 (PK_{A_1})^{k_1} (\bmod p).$$

While, the ciphertext of m_2 is

$$C_1^1 \equiv g^{k_2} (\bmod p) \text{ and } C_2^1 \equiv m_2 (PK_{A_2})^{k_2} (\bmod p).$$

•

.

.

and the ciphertext of m_n is

$$C_1^h \equiv g^{k_n} (\bmod p) \text{ and } C_2^h \equiv m_n (PK_{A_n})^{k_n} (\bmod p).$$

The ciphertext $(C_1, C_2), (C_1^1, C_2^1), (C_1^2, C_2^2), \ldots, (C_1^h, C_2^h)$ is sent to first user. The ciphertext in the PD-EPKC can be represented as the network system as shown in Figure (3.35).

The PD-EPKC consists of n paths, the first contains the C_1 and C_2 of m_1 and the second consists C_1^1 and C_2^1 of m_2 and the last contains C_1^h and C_2^h of m_n. The reliability of the proposed PD-EPKC can be determined using modified pivotal decomposition method. Applying the law of total probability involves selecting a component and then calculating the reliability of the system in two partial cases, if the component fails, the change is done by deleting the path and creating a new path and calculate the reliability of the system with the success of the new component as follows.

Step1. A keystone component is first chosen. Here, the component C_i represents as the keystone component.

Step2. A component C_i can be successful or failure. If C_2 is failure, then the path is deleted. The reliability of system given by

R(system success/component C_i failure) = P(system success/component C_i failure)

The scheme of encrypted plaintext Fig (3.35) transformed into Fig. (4.22)

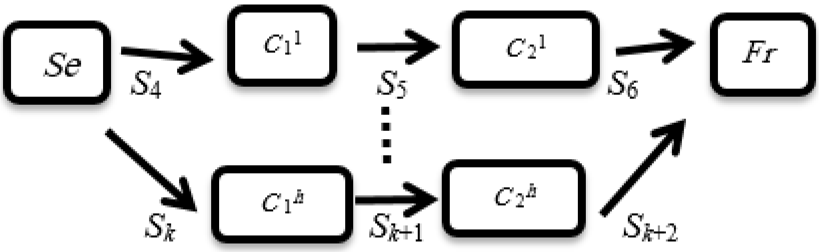


Figure 4.22. Network system of in *n*-dimension after deleted one path.

New alternative path of deleted path C_i is created to compute new C_i^{h+1} through choosing $k_i^{'}$ the ciphertext $C = (C_1^{h+1}, C_2^{h+1})$

$$C_1^{h+1} \equiv g^{k_i^{'}} (\bmod p) \text{ and } C_2^{h+1} \equiv m_i (Pk_{A_i})^{k_i^{'}} (\bmod p).$$

So, a pair of the ciphertext (C_1^{h+1}, C_2^{h+1}) is sent to first user.

The scheme of encrypted messages after delete and change the path in Figure (4.22) transformed into Figure (4.23).

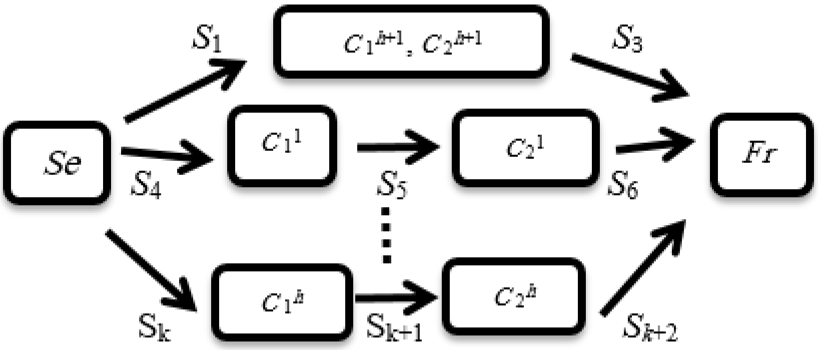


Figure 4.23. Network system in *n* dimension of the (C_1^{h+1}, C_2^{h+1}) updated path.

The reliability of system when component C_i^{h+1} is successful

$$R \text{ (system success/component } C_i^{h+1} \text{ is successful)}$$

$$= P\text{(system success/component } C_1^{h+1} \text{ is successful)} .$$

First user receives the ciphertext (C_1^{h+1}, C_2^{h+1}), (C_1^1, C_2^1) and (C_1^h, C_2^h) so she/he wants to decrypt it and recover the plaintext m_1, through the following calculation

$$m_i \equiv ((C_1^{h+1})^{a_i})^{-1} \times C_2^{h+1} (\bmod p).$$

and recover the plaintext m_2,

$$m_2 \equiv ((C_1^1)^{a_2})^{-1} \times C_2^1 (\bmod p).$$

While, recover the plaintext m_n,

$$m_n \equiv ((C_1^h)^{a_n})^{-1} \times C_2^h (\bmod p).$$

The reliability of system when component C_i failure and component C_i^{h+1} successful

$R_S = p_i$ (R system success/component C_i^{h+1}success) + q_i(R(system success/component C_i failure).

4.3.2 The Pivotal decompose of *n*-Dimension RSA Public Key Cryptosystem.

This section proposes the *n*-dimension of RSA public key cryptosystem which is called reliable RSA cryptosystem (PD-RSA). The domain parameters of PD-RSA are: $p_1, p_2, ..., p_n$ and $q_1, q_2, \ldots, q_n$ are large secret primes and e is a public encryption exponent with the property that gcd(e, (p_i-1)(q_i-1)) = 1, which are selected by first user. She/He computes her/his public modulus $N_i = p_i q_i$, and compute Ø(N_i) = (p_i-1)(q_i-1), i =1,2,…,n. First user sends the public key (N_i, e) to the second user.

Second user wants to encrypt his/her plaintext M =($m_1, m_2, \ldots, m_n$). He/She first chooses his/her plaintext M and divides it into n parts $m_1, .., m_n \in [1, N_i\text{-}1]$.

He/She uses first user's public key (N_i, e) to compute the ciphertext $C = (C_1, \ldots, C_h)$ of $m_1, m_2, \ldots, m_n$ respectively, where h number of the ciphertext by

$$C_1 \equiv m_1^e (\bmod N_1),\ C_2 \equiv m_2^e (\bmod N_2),\ \ldots,\ C_h \equiv m_n^e (\bmod N_n).$$

The ciphertext ($C_1, \ldots, C_h$) is sent to first user as the network of the ciphertext ($C_1, \ldots, C_h$) and public parameters N_i as shown in Figure (3.40). First user after receiving the network cryptosystem, he/she discusses the ciphertext in Figure (3.40) as follows. The PD-RSA consists of n paths, the first path contains the N_1 and C_1 of m_1 and the second path contains N_2 and C_2 of m_2 and the last path contains N_n and C_h of m_n. The reliability of the proposed PD-RSA can be determined using modified decomposition method. Applying the law of total probability involves selecting a component and then calculating the reliability of the system in two partial cases, if the component fails, the change is done by deleting the path and creating a new path and calculate the reliability of the system with the success of the new component as follows.

Step1: A keystone component is chosen first. Here, component N_1 represents as the keystone component.

Step2: A component N_1 can be successful or failure. If it is failure, then the path is deleted. The reliability of system given by

$$R(\text{system success/component } N_1 \text{ failure})$$

$$= P(\text{system success/component } N_1 \text{ failure})$$

The scheme of encrypted plaintext in Figure (3.40) transformed into Figure (4.24)

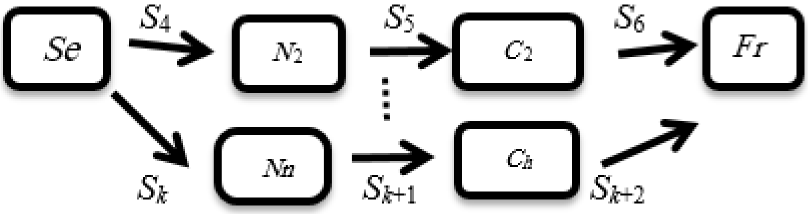


Figure 4.24. Network system of PD-RSA in n dimension.

New alternative path of deleted path C_i or N_i is created to compute new C_i' or N_i' through choosing p_i', q_i' where $N_i' = p_i' \times q_i'$ and $\text{Ø}(N_i') = (p_i' -1)(q_i' -1)$ the ciphertext

$$C_i^{'} \equiv m_i^e (\bmod p)$$

So, a pair of the ciphertext $C_i^{'}$ is sent to first user.

The scheme of encrypted plaintext after delete and change the path in Figure (4.22) transformed into Figure (4.25).

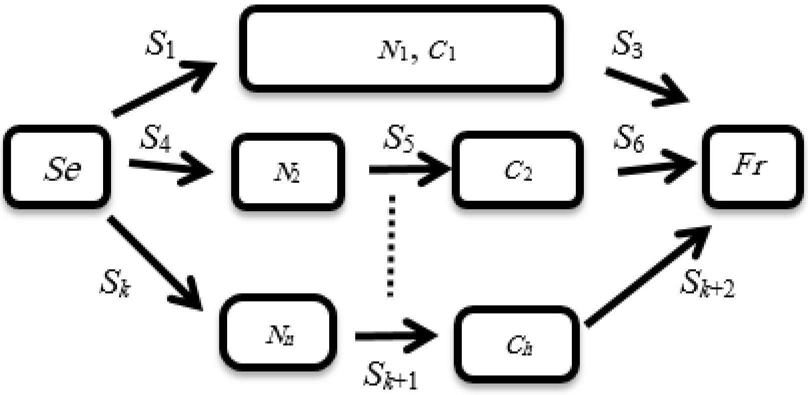


Figure 4.25. Network system of PD-RSA updated in *n* dimension.

The reliability of system when component $C_i^{'}$ is successful

R (system success/ component $C_i^{'}$ is successful)

= P(system success/ component $C_i^{'}$ is successful).

Upon first user receives the ciphertext, she/ he want to decrypt the ciphertext and recover the original plaintext. So, She/ He calculates the following steps. First User knows Ø(N_1) = (p_1-1)(q_1-1), Ø($N_2^{'}$) = ($p_2^{'}$-1)($q_2^{'}$-1), so $ed_i \equiv 1 \bmod (p_i\text{-}1)(q_i\text{-}1)$ for i=1,2 can be solved, namely

$$d_i^{'} \equiv e^{-1} (\bmod Ø(N_i^{'}))$$

and

$$d_2 \equiv e^{-1} \bmod(Ø(N_2))$$

While,

$$d_n \equiv e^{-1} \bmod(Ø(N_n))$$

First user also calculates

$$m_i \equiv (C_i^{'})^{d_i^{'}} (\bmod N_i^{'})$$

and

$$m_2 \equiv (C_2^{d_2} (\bmod N_2)$$

While,

$$m_n \equiv (C_n^{d_n} (\bmod N_n)$$

The reliability of system when component C_i failure and component $C_i^{'}$ successful

$R_S = p_i\,(R$(system success/component $C_i^{'}$ success) + $q_i(R$(system success/component C_i failure).

4.3.3 The Reliable of *n*-Dimension Rabin Public Key Cryptosystem.

The alternative version the Rabin Cryptosystem (RPKC) is proposed with n dimension. It is computationally secure in compare with the original one. On proposed RPKC which is also called reliable Rabin public key cryptosystem (PD-RPKC), first user selects the parameters: $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_n$ as a large secret primes, where p_l and $q_l \equiv 3 \pmod 4$ with $p_l \neq q_l$. First user also computes her/his public modulus's $n_l = p_l q_l$. She/He keeps the private keys p_l and q_l. Second user knows the public keys n_l. The plaintext M is chosen and divided into n parts m_l, where $m_l \in F_{n_l}^{*}$, $l = 1,2, \ldots, n$. He/She computes his/her ciphertext C_h, h is number of ciphertext.

$$C_h \equiv m_l^2 (\bmod n_l)$$

The ciphertext C_h can be represented as the network system as shown in Figure (3.45). The idea with n preivous cryptosystem will be applied. n paths on the R-RPKC have been created. First one contains the C_1 of m_1 and the second one contains C_2 of m_2 and last one contains C_h of m_n. The reliability of the proposed PD-RPKC can be determined using modified pivotal decomposition method. Applying the law of total probability involves selecting a component and then calculating the reliability of the system in two partial cases, if the component fails, the change is done by deleting the path and creating a new path and calculate the reliability of the system with the success of the new component as follows.

Step1: A keystone component is choses first. Here, the component C_i represents as the keystone component.

Step2: A component C_i can be successful or failure. If C_i is failure, then the path is deleted. The reliability of system given by

$$R(\text{system success/component } C_i \text{ failure})$$

$$= P(\text{system success/component } C_i \text{ failure})$$

The scheme of encrypted messages in Figure (3.45) transformed into Figure (4.26)

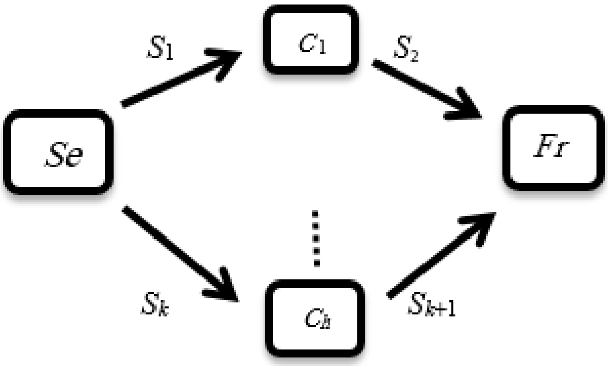


Figure 4.26. Network system of ciphertext in n dimension after deleted one path.

New alternative path of deleted path C_i is created to compute new $C_i^{'}$ through choosing $p_i^{'}$ and $q_i^{'}$ where p_i, $q_i \equiv 3 \pmod 4$ and $p_i \neq q_i$, with $n_i = p_i q_i$. The ciphertext $C_i^{'}$ is computed by

$$C_i^{'} \equiv m_i \,(\text{mod}\, n_i^{'}).$$

The scheme of encrypted messages after delete and change the path in Figure (4.24) transformed into Figure (4.27).

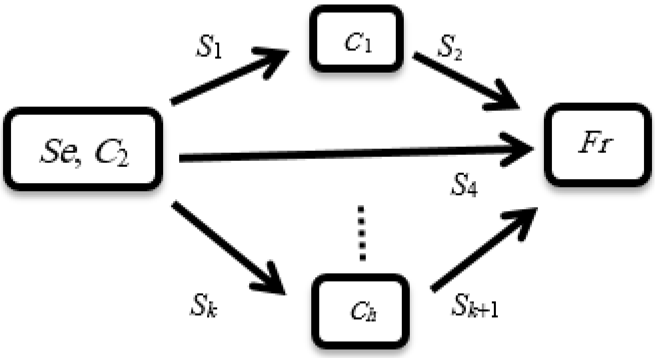


Figure 4.27. Network system of encrypted plaintexts with updated one path.

The reliability of system when component $C_i^{'}$ is successful

R (system success/component $C_i^{'}$ is successful)

= P(system success/component $C_1^{'}$ is successful).

By applying the steps above, we obtain the original plaintext. First user wants decryption ciphertext, she/he knows the prime factors p_l, q_l of n_l respectively, She/he solves the following two congruence's

$$(m_l p_l)^2 \equiv C_h (\text{mod}\, p_l) \text{ and } (m_l q_l)^2 \equiv C_h (\text{mod}\, q_l).$$

She/He uses the Euler's criterion to determine if C_h is a quadratic residue modulo p_l (and modulo q_l) or not. When $p_l \equiv 3 \pmod 4$, there is a simple formula to compute square roots of quadratic residues modulo p_l. Suppose C_h is a quadratic residue modulo p_l, where $p_l \equiv 3 \pmod 4$. Then we have that

$$\left(\pm C_h{}^{(p_l+1)/4}\right)^2 \equiv C_h{}^{(p_l+1)/2}\ (mod\ p_l)$$
$$\equiv C_h{}^{(p-1)/2} C_h\ (mod\ p_l)$$
$$\equiv C_h\ (mod\ p_l).$$

If C_h is a quadratic residue modulo p_l, then $C_h{}^{(p_l-1)/2} \equiv 1$ (mod p_l). Hence, two square roots of C_h modulo p_i are $a = \pm C_h{}^{(p_l+1)/4}$ mod p_l. In a similar fashion, two square roots of C_h modulo q_l are $b = \pm C_h{}^{(q_l+1)/4}$ mod q_l, with m_l has (+a, +b), (+a, -b), (-a, +b), (-a, -b), l = 1,2, …, n and h is number of ciphertext. This congruence's are solved using the Chinese remainder theorem (CRT). The reliability of system when component C_i failure and component C_i' successful

$R_S = p_i$ (R(system success/component C_i' success) + q_i(R(system success/component C_i failure).

4.4 Security Considerations for the proposed Asymmetric Cryptosystem.

The security of the proposed reliable public key cryptosystem type El-Gamal is based on the difficulty for solving the discrete logarithm problem (DLP). To recover the private keys, an adversary needs to compute $a_1 = \mathrm{DLP}_{g,p}(PK_{A1})$ and $a_2 = \mathrm{DLP}_{g,p}(PK_{A2})$ which are used to compute $((C_1)^{a_1})^{-1}$ and $((C_1')^{a_2})^{-1}$ that represent as the first parts for recovering m_1 and m_2 respectively. On the other hand, for determining the random numbers k_1 and k_2, it requires to compute $k_1 = \mathrm{DLP}_{g,p}(C_2)$ and $k_2 = \mathrm{DLP}_{g,p}(C_2')$ which also represent the DLP. These calculations are infeasible if p is at least 2×300 decimal digits and p-1 has at least one large prime factor. Another version of RSA and Rabin is proposed to enhance the security. On new proposed cryptosystem which is named by R-RSA and R-RC cryptosystem, two parameters N_1 and N_2 of public key are generated based on secret primes p_1q_1 and p_2q_2 respectively. So, we are working with two integer factorization problems which are considered as hard mathematical problem to solve by attackers with large choice of primes. Thus, it is more difficult to get these primes that the attacker can be used to recover two parts of the plaintext. Moreover, the three proposed systems with pivotal decomposition give the new algorithms high security protection in data transmission.

Chapter Five

Conclusions and Future Works

5.1 Conclusions

New versions of asymmetric cryptosystem algorithms say El-Gamal, RSA and Rabin are proposed in this work. The proposed cryptosystems used the reliability systems and some reliable methods to increase the security in two dimension. The R-EPKC, R-RSA and R-Rabin with 2-dimension are applied first using the reliable path tracing method for encryption process and reliable serial-parallel reduction method to decrypt the ciphertext and recover the original plaintext. The reliable modified pivotal decomposition method also is used to draw other versions of El-Gamal, RSA and Rabin cryptosystems. The *n* dimension of these cryptosystems is proposed in this work as well. The keys are generated in *n* dimensions. The plaintext is chosen as the texts, word or numbers that is divided into *n* parts. The ciphertext of each part is computed independently. The reliability and efficiency are determined with path tracing, serial-parallel reduction and modified pivotal decomposition methods. The last method is considered as safe method to resist any attacker tries break down any path and create another alternative path with a new private key and a new ciphertext. No doubt time complexity is increased, but it is negligible in compare to security level and protection of plaintext which is more important in information security.

5.2 Future works:

Some suggestions can be considered as the future works:

1. Using other reliable methods to determine the reliability, efficiency and security of the cryptosystems.

2. With same reliable methods that are used in this work, it is possible to modify other kinds of asymmetric cryptosystems for increasing their security.

3. Reliability allocation to the proposed algorithms.

References

[1] Singh, R., Pavan Kumar, C., & Selvakumar, R. (2019). Encode-then-Encrypt: A Novel Framework for Reliable and Secure Communication. In *Applied Mathematics and Scientific Computing: International Conference on Advances in Mathematical Sciences, Vellore, India, December 2017-Volume II* (pp. 581-594). Springer International Publishing.

[2] Zaidan, B. B., Zaidan, A. A., Al-Frajat, A. K., & Jalab, H. A. (2010). On the differences between hiding information and cryptography techniques: An overview. *Journal of Applied Sciences*, *10*(15), 1650-1655.

[3] Breveglieri, L. (Ed.). (2006). *Fault Diagnosis and Tolerance in Cryptography: Third International Workshop, FDTC 2006, Yokohama, Japan, October 10, 2006, Proceedings* (Vol. 4236). Springer Science & Business Media.

[4] Iaremchuk, I. E. (2013). Evaluation of cryptographic reliability of information encryption methods based on recurrent sequences. *Eastern-European Journal of Enterprise Technologies*, *2*, 10-62.

[5] Xiao, S., Gong, W., Towsley, D., Zhang, Q., & Zhu, T. (2014, June). Reliability analysis for cryptographic key management. In *2014 IEEE International Conference on Communications (ICC)* (pp. 999-1004). IEEE.

[6] Ahmadi, M., Vali, M., Moghaddam, F., Hakemi, A., & Madadipouya, K. (2015). A Reliable User Authentication and Data Protection Model in Cloud Computing Environments. *arXiv preprint arXiv:1508.01703*.

[7] Subramanian, S., Mozaffari-Kermani, M., Azarderakhsh, R., & Nojoumian, M. (2017). Reliable hardware architectures for cryptographic block ciphers LED and HIGHT. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *36*(10), 1750-1758.

[8] ÇALKAVUR, S. (2021). A New Public-Key Cryptosystem Based on LCD Codes. *Avrupa Bilim ve Teknoloji Dergisi*, (28), 320-324.

[9] Akhatov, A. R., Sabharwal, M., Nazarov, F. M., & Rashidov, A. (2022, April). Application of cryptographic methods to blockchain technology to increase data reliability. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 642-647). IEEE.

[10] Stapelberg, R. F. (2009). *Availability and maintainability in engineering design* (pp. 295-527). Springer London.

[11] Aven, T., & Jensen, U. (Eds.). (1999). *Stochastic models in reliability*. New York, NY: Springer New York.

[12] Chowdhury, A., & Koval, D. (2011). *Power distribution system reliability: practical methods and applications*. John Wiley & Sons.

[13] Dhillon, B. S. (2006). *Maintainability, maintenance, and reliability for engineers*. CRC press.

[14] Rausand, M. (2014). *Reliability of safety-critical systems: theory and applications*. John Wiley & Sons.

[15] Zio, E. (2007). *An introduction to the basics of reliability and risk analysis* (Vol. 13). World scientific.

[16] Fazlollahtabar, H., & Niaki, S. T. A. (2017). *Reliability Models of Complex Systems for Robots and Automation*. CRC Press.

[17] Murthy, D. P., Rausand, M., & Østerås, T. (2008). *Product reliability: specification and performance*. Springer Science & Business Media.

[18] Ross, S. M. (2014). *Introduction to probability models*. Academic press.

[19] Yang, G. (2007). *Life cycle reliability engineering*. John Wiley & Sons.

[20] Kuo, W., & Zuo, M. J. (2003). *Optimal reliability modeling: principles and applications*. John Wiley & Sons.

[21] A. A. AL-Ali, "*Reliability of complex system*", Basra J. science, 16(1),115-112, Basra, Iraq, 1998 .

[22] Lafortune, E. P., & Willems, Y. D. (1993). Bi-directional path tracing.

[23] Fascione, L., Hanika, J., Pieké, R., Villemin, R., Hery, C., Gamito, M., ... & Mazzone, A. (2018). Path tracing in production. In *ACM SIGGRAPH 2018 Courses* (pp. 1-79).

[24] Kuo, W., & Zuo, M. J. (2003). *Optimal reliability modeling: principles and applications*. John Wiley & Sons.

[25] Christensen, C. (2010). Review of cryptography and network security: Principles and practice. *Cryptologia*, *35*(1), 97-99.

[26] Lidl, R., & Niederreiter, H. (1994). *Introduction to finite fields and their applications*. Cambridge university press.

[27] Silverman, J. H., Pipher, J., & Hoffstein, J. (2008). *An introduction to mathematical cryptography* (Vol. 1). Springer New York.

[28] Hankerson, D., & Menezes, A. (2021). Elliptic curve cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1-2). Berlin, Heidelberg: Springer Berlin Heidelberg.

[29] Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

[30] Stinson, D. R. (2005). *Cryptography: theory and practice*. Chapman and Hall/CRC.

[31] Kerl, J. (2004). Computation in finite fields. *Arizona State University and Lockheed Martin Corporation*, *1*(1), 1-84.

[32] Yang, C. C., Chang, T. Y., Li, J. W., & Hwang, M. S. (2003). Simple Generalized Group-Oriented Cryptosystems Using ElGamal Cryptosystem. *Informatica*, *14*(1), 111-120.

[33] Snyder, L. V., & Shen, Z. J. M. (2019). *Fundamentals of supply chain theory*. John Wiley & Sons.

[34] Toradmalle, D. K., Muthukuru, J., & Sathyanarayana, B. (2018). Cryptanalysis of an Improved ECDSA. *International Journal of Engineering Research and Technology, 11*(4), 615-619.

[35] Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., & Ikematsu, Y. (2021). *International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019* (p. 274). Springer Nature.

[36] Silverman, J. H., Pipher, J., & Hoffstein, J. (2008). *An introduction to mathematical cryptography* (Vol. 1). Springer New York.

[37] Singh, L. D., & Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, *54*, 73-82.

[38] Aumasson, J. P. (2017). *Serious cryptography: a practical introduction to modern encryption*. No Starch Press.

[39] Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014, November). A comparative survey of symmetric and asymmetric key cryptography. In *2014 international conference on electronics, communication and computational engineering (ICECCE)* (pp. 83-93). IEEE.

[40] Abood, Z. A., & Sadkhan, S. B. (2022, May). Security evaluation techniques of Cognitive Radio Network status and challenges. In *2022 5th International*

Conference on Engineering Technology and its Applications (IICETA) (pp. 265-270). IEEE.

[41] Delfs, H., Knebl, H., Delfs, H., & Knebl, H. (2015). Symmetric-key cryptography. *Introduction to Cryptography: Principles and Applications*, 11-48.

[42] Oppliger, R. (2021). *Cryptography 101: From Theory to Practice*. Artech House.

[43] Dissanayake, W. D. M. G. M. (2018). An improvement of the basic El-Gamal public key cryptosystem. *International Journal of Computer Applications Technology and Research*, *7*(2), 40-44.

[44] Katz, J., & Lindell, Y. (2007). *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC.

[45] Mollin, R. A. (2002). *RSA and public-key cryptography*. CRC Press.

[46] Hashim, H. R. (2014). H-Rabin cryptosystem. *Journal of Mathematics and Statistics*, *10*(3), 304.

Appendix A

Table ASCII Code

Dec.	Char.	Dec.	Char.	Dec.	Char.	Dec.	Char.
0	Null	32	Space	64	@	96	`
1	Start of heading	33	!	65	A	97	a
2	start of text	34	"	66	B	98	b
3	end of text	35	#	67	C	99	c
4	end of transmission	36	$	68	D	100	d
5	Enquiry	37	%	69	E	101	e
6	Acknowledge	38	&	70	F	102	f
7	Bell	39	'	71	G	103	g
8	Backspace	40	(	72	H	104	h
9	horizontal tab	41	)	73	I	105	i
10	NL line feed, new line	42	*	74	J	106	j
11	vertical tab	43	+	75	K	107	k
12	NP form feed, new page	44	,	76	L	108	l
13	carriage return	45	-	77	M	109	m
14	shift out	46	.	78	N	110	n
15	shift in	47	/	79	O	111	o
16	data link escape	48	0	80	P	112	p
17	device control 1	49	1	81	Q	113	q
18	device control 2	50	2	82	R	114	r
19	device control 3	51	3	83	S	115	s
20	device control 4	52	4	84	T	116	t
21	negative acknowledge	53	5	85	U	117	u
22	synchronous idle	54	6	86	V	118	v
23	end of trans. Block	55	7	87	W	119	w
24	Cancel	56	8	88	X	120	x
25	end of medium	57	9	89	Y	121	y
26	Substitute	58	:	90	Z	122	Z
27	Escape	59	;	91	[	123	{
28	file separator	60	<	92	\	124	|
29	group separator	61	=	93	]	125	}
30	record separator	62	>	94	^	126	~
31	unit separator	63	?	95	_	127	Del

الملخص

درجة الامن في الواقع مهمة للغاية وهي مصممة لضمان السرية من ناحية ومن ناحية أخرى الشفافية الكاملة للمعلومات، ترتبط الموثوقية بالتوافر والتي توصف بأنها قدرة المكون او النظام على العمل في لحظه او فترة زمنية محددة . في هذا الصدد، تهدف هذه الرسالة الى زيادة مستوى الأمان في خوارزميات التشفير غير المتماثلة ك EPKC, RSA, RPKC من خلال الاعتماد على مخططات وطرق الموثوقية. في هذا العمل تم اقتراح نسخه موثوقة EPKC, RSA, RPKC مع 2-dim. على نظام R-EPKC, R-RSA, R-RPKC النص العادي يقسم الى جزئيين m_1, m_2 يتم تشفير كل جزء بشكل مستقل لأنشاء مسارين من النص المقسم. النص العادي في R-EPKC, R-RSA, R-RPKC يمثل على شكل شبكي يحتوي مسارين الأول يحتوي النص المشفر ل m_1 والمسار الثاني يحتوي النص المشفر ل m_2 يتم تحديد موثوقية R-EPKC, R-RSA, R-RPKC بطريقه تتبع المسار PTM. يتم استخدام تقنيه جديده لدمج الرسائل المشفرة بأستخدام طريقه التخفيض PSRM التي يتم استخدامها لفك النص المشفر و استعاده النص الأصلي. اذا تعرض احد المسارين الى هجوم من قبل كاسر الشفرة يتم حذف المسار وانشاء مسار بديل مع نص مشفر جديد بأستخدام طريقه التحلل المحوري المعدلة M-PDM أيضا تم تعميم هذا الانظمة المقترحة ل n-dim. الهدف من تقسيم النص العادي الى أجزاء هو الحصول على موثوقية اعلى للنظام وبالتالي زيادة امان النظام بشكل افضل لانه حتى لو تمكن كاسر الشفرة من كسر احدى أجزاء الشفرات لن يتمكن من الحصول على جميع المعلومات في النص العادي الأصلي فقط جزء منه و بالتالي لن يستفيد من المعلومات التي حصل عليها. في الخوارزميات المفتاح العمومي يحتوي النص المشفر على مسار واحد فقط (سلسله) وفشل احد مكونات المسار يعني فشل النص المشفر. لكن بعد تقسيم النص العادي الى قسمين، سيصبح النظام متوازيا ولا يعني فشل جزء واحد من النظام فشل النظام بأكمله. تناقش النتائج التجريبية ل R-EPKC, R-RSA, R-RPKC كحاله دراسة المعلمات الصغيرة. R-EPKC, R-RSA, R-RPKC تعتبر اكثر امان للتشفير و الاتصالات مقارنة بالأصلية.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية التربية للعلوم الصرفة

قسم الرياضيات

موثوقية أنظمة التشفيرغير المتناظرة

رسالة

مقدمة الى مجلس كلية التربية للعلوم الصرفة في جامعة بابل جزء من متطلبات نيل درجة الماجستير في التربية / الرياضيات

من قبل

بان جاسم كاظم ديكان

بأشراف

أ.م.د. رومى كريم خضر عجينة

1445هـ 2023